Guia do Usuário do Nessus 5.2 HTML5

16 de janeiro de 2014

(Revisão 20)

Sumário

Introdução

Este documento descreve como usar a **interface do usuário Nessus (IU)** do Tenable Network Security. Envie seus comentários e sugestões para support@tenable.com.

A interface do usuário Nessus é uma interface baseada na Web que complementa o scanner de vulnerabilidades Nessus. Para usar a IU, é preciso um scanner Nessus em operação instalado e estar familiarizado com o seu uso.

Padrões e convenções

Em toda a documentação, os nomes de arquivos, daemons e executáveis são indicados com a fonte **`courier bold`**, como **`gunzip`**, **`httpd`** e **`/etc/passwd`**.

As opções de linhas de comando e palavras-chave também são indicadas com a fonte **`courier bold`**. Os exemplos de linhas de comando podem ou não conter o prompt da linha de comando e o texto gerado pelos resultados do comando. Os exemplos de linhas de comando exibirão o comando executado em **`courier bold`** para indicar o que o usuário digitou, enquanto que o exemplo de saída gerado pelo sistema será indicado em `courier` (sem negrito). Um exemplo da execução do comando **`pwd`** do Unix é apresentado a seguir:

```
# pwd
/opt/nessus/
#
```

As observações e considerações importantes são destacadas com este símbolo e caixas de texto escurecidas.

As dicas, exemplos e práticas recomendadas são destacados com este símbolo e texto branco sobre fundo azul.

O que há de novo no Nessus 5.2

A partir de 22 de agosto de 2013, os nomes de produtos Nessus foram revisados como mostrado abaixo:

Nome anterior do produto	Novo nome do produto
Nessus ProfessionalFeed	Nessus
Nessus HomeFeed	Nessus Home

A lista a seguir mostra os nomes de produtos oficiais da Nessus:

- Nessus®
- Serviço de Perímetro Nessus
- Nessus Auditor Bundles
- Nessus Home

Visão geral da interface do usuário (IU) Nessus

Descrição

A interface do usuário (IU) Nessus é uma interface baseada na Web desenvolvida para o scanner Nessus, que consiste em um servidor HTTP simples e um cliente da Web, e dispensa a instalação de qualquer software além do servidor Nessus. A partir do Nessus 4, todas as plataformas aproveitam o mesmo código básico, eliminando a maioria dos erros específicos de plataforma e acelerando a implementação de novos recursos. Os recursos principais são:

- Gera arquivos **`.nessus`** usados pelos produtos da Tenable como padrão de dados de vulnerabilidades e políticas de varredura.
- Uma sessão de política, lista de alvos e os resultados de várias varreduras podem ser armazenados em um único arquivo **`.nessus`** que pode ser facilmente exportado. Consulte o guia "Nessus v2 File Format" (Formato de arquivo Nessus v2)" para mais detalhes.
- A interface do usuário exibe, em tempo real, os resultados das varreduras, de modo que não é preciso esperar a conclusão de uma varredura para ver os resultados.
- Unifica a interface do scanner Nessus, independentemente da plataforma de base. As mesmas funções existem no Mac OS X, Windows e Linux.
- As varreduras continuarão sendo executadas no servidor, mesmo se o usuário for desconectado por qualquer motivo.
- Os relatórios de varredura do Nessus podem ser carregados por meio da interface do usuário Nessus e comparados a outros relatórios.
- Um assistente de política para ajudar a criar rapidamente políticas de varredura eficientes para realizar auditoria da rede.

Plataformas compatíveis

Como a interface do usuário Nessus é um cliente da Web, ela funciona em qualquer plataforma com um navegador moderno.

A interface do usuário baseada na Web do Nessus é melhor aproveitada usando o navegador Microsoft Internet Explorer 10, Mozilla Firefox 24, Google Chrome 29, Opera 16 ou Apple Safari 6 na área de trabalho. Além disso, o Nessus é compatível com o Chrome 29 para Android, bem como com navegadores no iOS 7.

A interface do usuário baseada na Web do Nessus requer no mínimo a versão 9 do Microsoft Internet Explorer.

Instalação

O gerenciamento do servidor Nessus 5 pelo usuário é realizado somente por uma interface baseada na Web ou pelo SecurityCenter. O NessusClient independente anterior não é mais atualizado nem tem suporte.

Consulte o "Nessus 5.2 Installation and Configuration Guide" (Guia de Instalação e Configuração do Nessus 5.2) para obter instruções sobre como instalar o Nessus. A partir do Nessus 5.0, Oracle Java (conhecido como Java da Sun Microsystems) é necessário para a funcionalidade de relatórios no formato PDF.

Operação

Visão geral

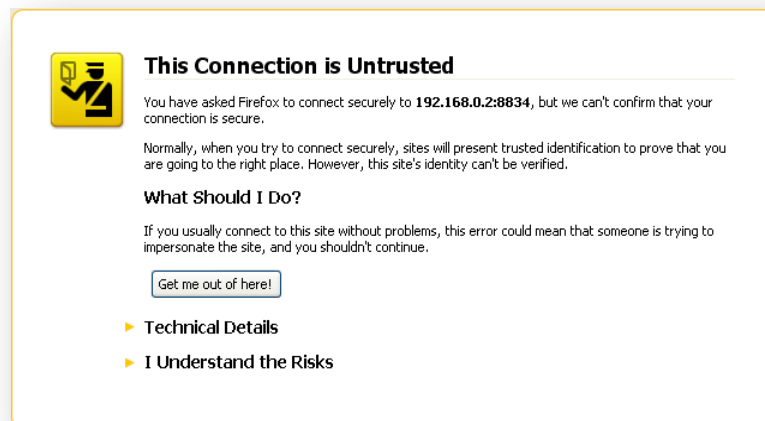
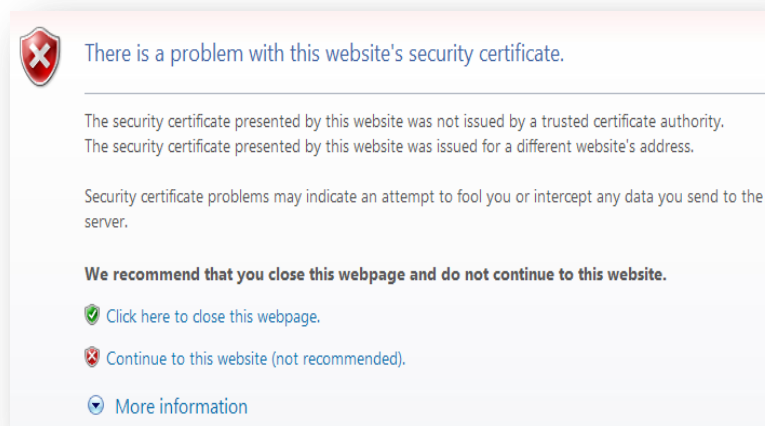
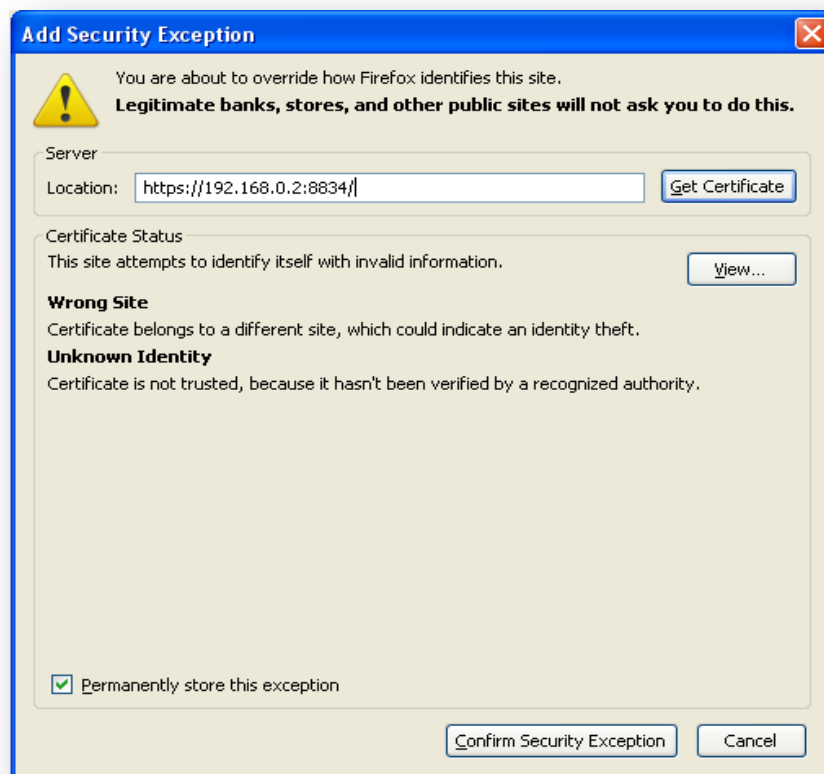
O Nessus oferece uma interface simples, mas poderosa, para gerenciar as atividades de varredura de vulnerabilidades.

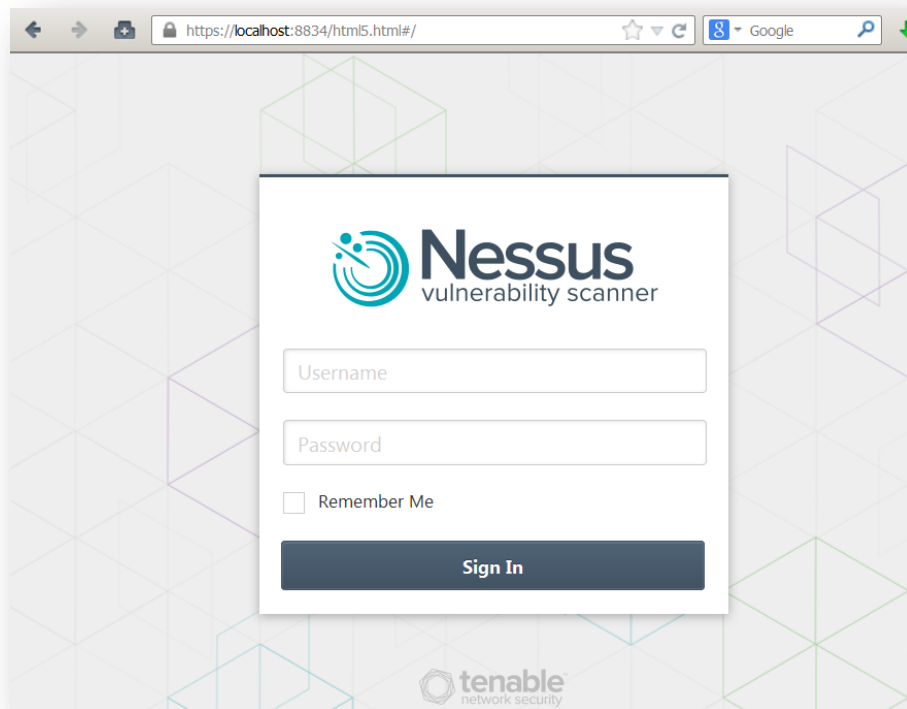
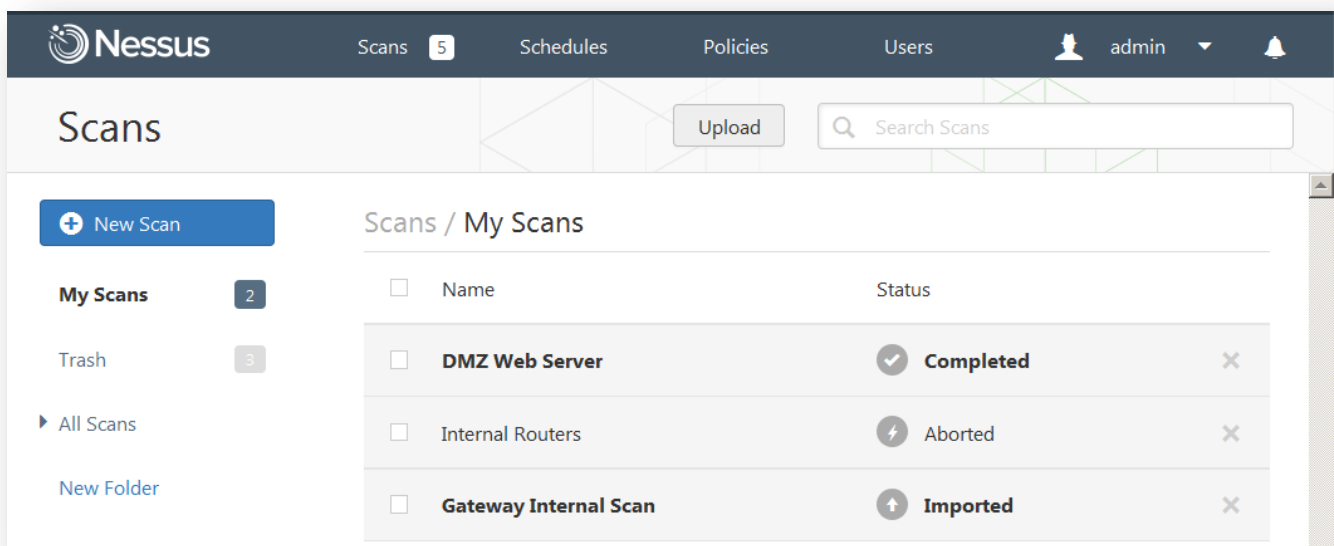
Conexão com a IU do Nessus

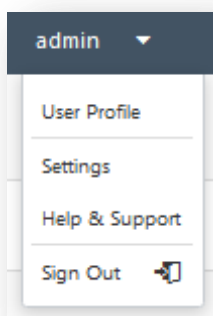
Para iniciar a IU HTML5 do Nessus, faça o seguinte:

- Abra o navegador de sua preferência.
- Digite `https://[server IP]:8834/` na barra de navegação.

Certifique-se de se conectar à interface do usuário por meio de HTTPS, pois não são permitidas conexões HTTP sem criptografia.

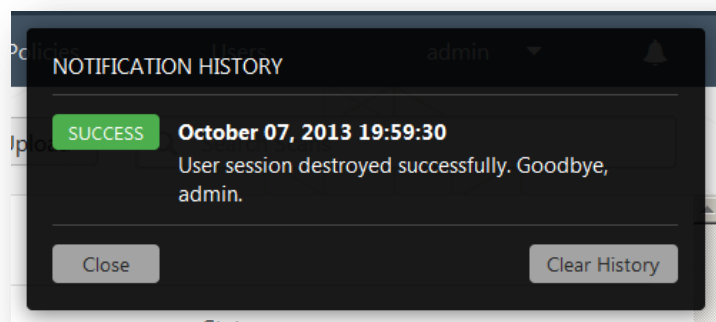
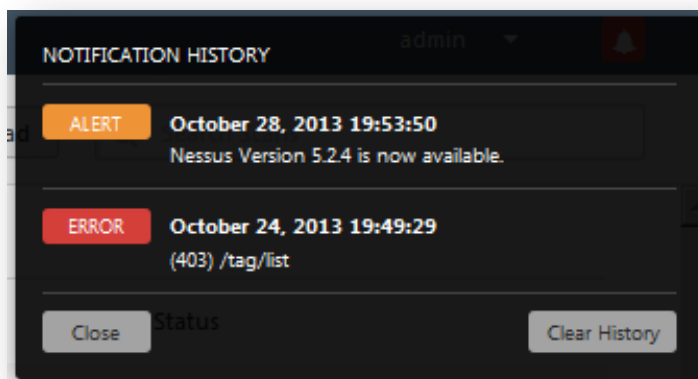
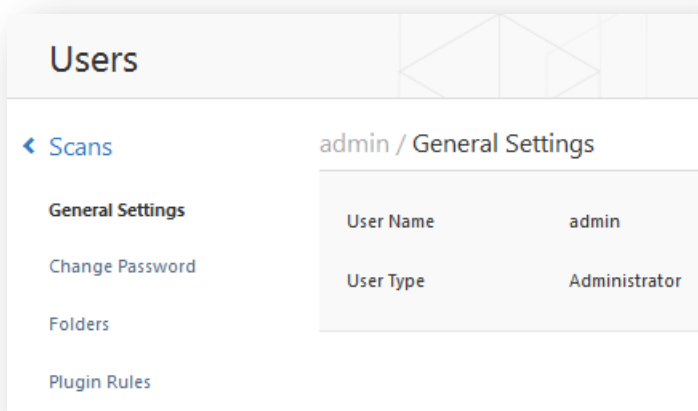
Ao tentar se conectar à interface do usuário Nessus pela primeira vez, a maioria dos navegadores exibirá um erro indicando que o site não é confiável, devido ao certificado SSL autoassinado:

Os usuários do Microsoft Internet Explorer podem clicar em "**Prosseguir para o Website (não recomendado)**" para carregar a interface do usuário Nessus. Os usuários do Firefox 3.x podem clicar em "**Entendo os riscos**" e, depois, em "**Adicionar exceção...**" para abrir a caixa de diálogo de exceções de sites:

Verifique se a barra "Endereço:" reflete o URL do servidor Nessus e clique em "**Confirmar exceção de segurança**". Para obter informações sobre como instalar um certificado SSL personalizado, consulte o "Nessus 5.2 Installation and Configuration Guide" (Guia de Instalação e Configuração do Nessus).

Depois que o navegador confirmar a exceção, a seguinte tela de abertura será exibida:

Autentique-se usando a conta e senha de administrador criadas anteriormente, durante o processo de instalação. Ao fazer login, você pode opcionalmente instruir o navegador a se lembrar do nome de usuário naquele computador. Use essa opção somente se o computador estiver sempre em um local seguro! Após a autenticação bem-sucedida, a interface do usuário exibirá os menus para procurar relatórios, realizar varreduras e gerenciar políticas. Os usuários com status de administrator também terão opções para gerenciamento de usuários e configuração do scanner Nessus:

Em qualquer ponto durante o uso do Nessus, as opções no menu superior esquerdo estarão presentes. A notação “admin” vista no canto superior direito da captura de tela acima denota a conta atualmente conectada, um menu suspenso e um sino para acesso rápido a notificações importantes relacionadas à operação do Nessus:

Ao clicar na seta suspensa, aparecerá um menu contendo opções para acessar o perfil de usuário, as configurações gerais do Nessus, informações sobre a instalação, opções de ajuda e suporte e uma opção para desconectar.

A opção “**User Profile**” (Perfil do usuário) abrirá um menu com várias páginas de opções relacionadas à conta do usuário, incluindo a função de troca de senha, o gerenciamento de pasta e a página de regras de plugins. Mais informações sobre essas opções podem ser encontradas abaixo.

A opção “**Settings**” (Configurações) oferece acesso à página “**About**” (Sobre), às opções de configuração do servidor de correio (se for administrador), feed de plugin (se for administrador) e opções avançadas de varredura (se for administrador). Mais informações sobre essas opções podem ser encontradas a seguir.

O link “**Help & Support**” (Ajuda e suporte) carregará a página de suporte da Tenable em uma nova guia ou janela. “**Sign Out**” (Desconectar) encerrará a sessão atual do Nessus.

Você pode clicar no ícone do sino no canto superior direito para exibir mensagens relacionadas às operações do Nessus, incluindo erros, notificação de novas versões do Nessus, eventos da sessão e etc.:

Ele também servirá como local para fornecer alertas ou erros adicionais através de janelas pop-up que desaparecerão logo depois e permanecerão no histórico de notificações até que sejam removidos:

Perfil do usuário
As opões do perfil do usuário permitem manipular opções relacionadas à conta.

O campo "**General Settings**" (Configurações gerais) mostra o usuário atualmente autenticado, bem como o tipo de usuário, se é Administrador ou não.

A opção "**Change Password**" (Alterar senha) permite alterar a senha, o que é recomendado fazer a cada 3 meses.

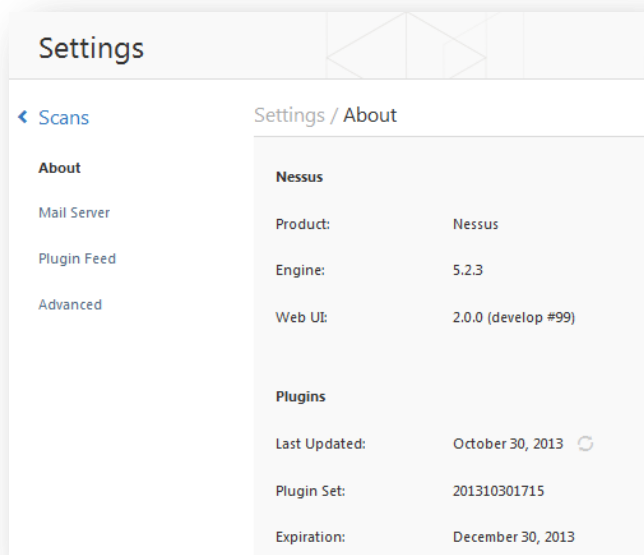
A opção "**Folders**" (Pastas) permite o gerenciamento de pastas para armazenar resultados de varreduras. Isso oferece um método para organizar e armazenar resultados de varredura para facilitar o gerenciamento.

A opção "**Plugin Rules**" (Regras de plugin) disponibiliza uma função para criar um conjunto de regras que ditam o comportamento de certos plugins relacionados à qualquer varredura realizada. Uma regra pode ser baseada no Host (ou todos os hosts), no ID do Plugin, em uma data de expiração opcional e na manipulação de Gravidade. As mesmas regras podem ser definidas na página de resultados da varredura.

Configurações
A seção "About" (Sobre) fornece informações relacionadas à instalação do Nessus, incluindo a versão do mecanismo, a versão da IU da Web, a data de atualização do plugin, a versão do conjunto de plugins e a data de expiração do feed.

A configuração "Mail Server" (Servidor de correio) controla as configurações relacionadas ao servidor SMTP. Para obter mais informações, consulte o "Nessus 5.2 Installation and Configuration Guide" (Guia de instalação e configuração do Nessus 5.2).

A configuração “Plugin Feed” (Feed de plugin) permite designar um host personalizado de atualização de plugins (por exemplo, para atualizações off-line a partir de um servidor interno central) e um proxy para atualizações de plugin. Para obter mais informações, consulte o “ Nessus 5.2 Installation and Configuration Guide” (Guia de instalação e configuração do Nessus 5.2).

A seção “Advanced” (Avançado) contém uma grande variedade de opções de configuração que oferecem um controle mais granular sobre o funcionamento do scanner. Para obter mais informações, consulte o “Nessus 5.2 Installation and Configuration Guide” (Guia de instalação e configuração do Nessus 5.2).

Atalhos da interface

A interface HTML5 tem diversos atalhos que permitem a navegação rápida, usando o teclado, para as seções principais da interface, bem como para a realização de atividades comuns. Podem ser usados em qualquer ocasião, a partir de qualquer lugar na interface:

Interface principal	
R	Results (Resultados)
S	Scans (Varreduras)
T	Templates (Modelos)
P	Policies (Políticas)
U	Users (Usuários)
C	Configuration (Configuração)
Shift + Seta para esquerda/direita	Alterna tabulações para esquerda ou direita

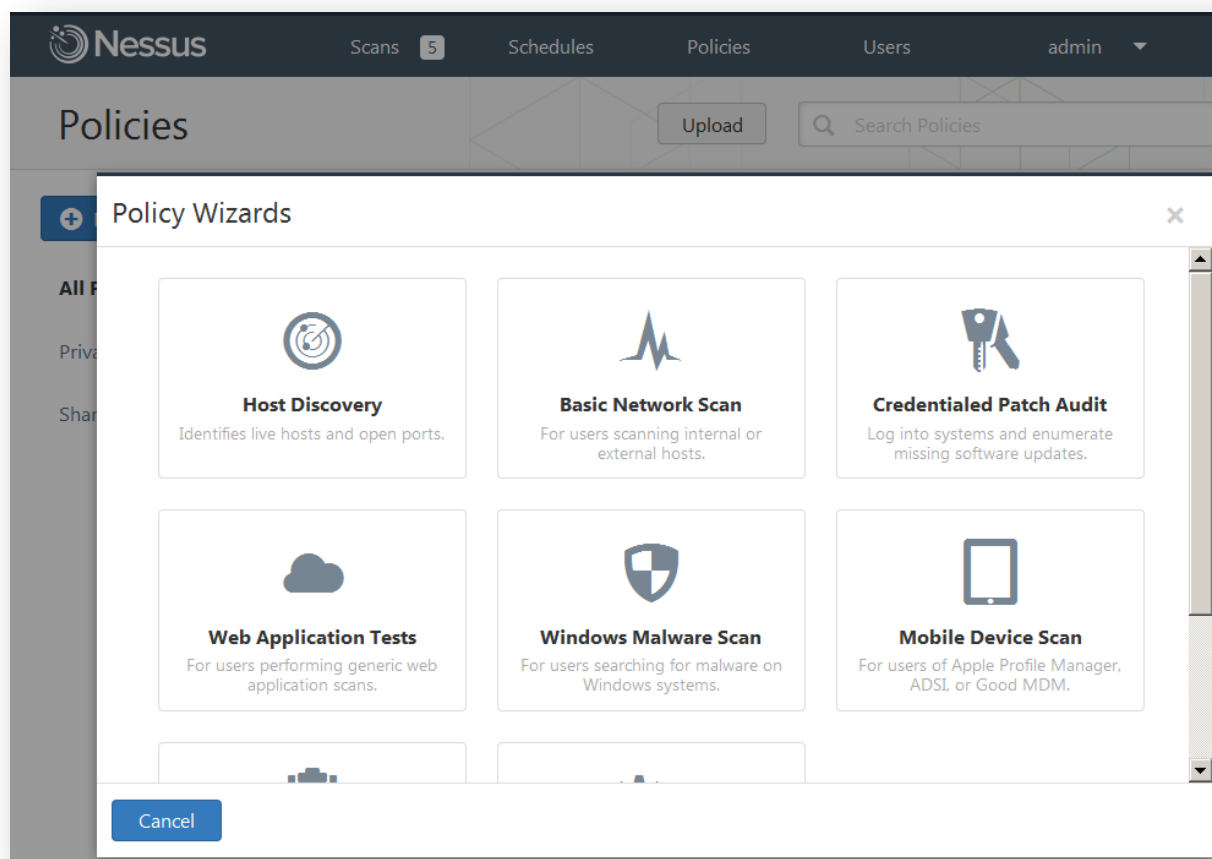
Shift + S	New Scan (Nova varredura)
Exibições de lista	
Shift + Seta para cima/baixo	Move a seleção para cima ou para baixo
Shift + Enter	Abre a entrada selecionada
Exibição de resultados	
Shift + U	(Upload Report) Upload de relatório
Esc	Voltar à exibição de resultados
Seta para esquerda/direita	Vulnerabilidade próxima/anterior em modo de detalhes
D	Excluir resultado selecionado
Exibição de varredura	
N	New Scan (Nova varredura)
Exibição de políticas	
Shift + U	Upload New Policy (Upload de nova política)
Exibição de usuário	
N	New User (Novo usuário)

Visão geral das políticas

Uma política do Nessus consiste em opções de configuração relacionadas à realização de uma varredura de vulnerabilidades. Algumas das opções são, entre outras:

- Parâmetros que controlam aspectos técnicos da varredura, como intervalos de tempo, número de hosts, tipo de varredura de porta etc.
- Credenciais para varreduras locais (por exemplo: Windows, SSH), varreduras autenticadas de bancos de dados Oracle, HTTP, FTP, POP, IMAP ou autenticação baseada em Kerberos.
- Especificações individualizadas de varreduras por família ou plugin.
- Verificações de políticas de conformidade de bancos de dados, detalhamento de relatório, configurações de varredura de detecção de serviços, verificações de conformidade Unix, entre outras opções.

Como criar uma nova política

Depois de se conectar à interface do usuário do servidor Nessus, é possível criar uma política personalizada ao clicar na opção "**Policies**" (Políticas) na barra superior e, em seguida, no botão "**+ New Policy**" (+ Nova política) à esquerda. A tela de adição de política é exibida como no exemplo a seguir:

Como usar o assistente de política

A primeira opção é usar o "Policy Wizard" (Assistente de política) para auxiliar na formação de uma política com uma finalidade específica. Os modelos padrão do assistente são:

Nome do "Policy Wizard" (Assistente de política)	Descrição
Host Discovery (Descoberta de host)	Identifica hosts ativos e portas abertas.
Basic Network Scan (Varredura básica de rede)	Para usuários fazendo varredura de hosts internos ou externos.
Credentialed Patch Audit (Auditoria de patch credenciado)	Faz login em sistemas e enumera atualizações de software ausentes.
Web Application Tests (Testes de aplicativos da	Para usuários fazendo varreduras em aplicativos genéricos da Web.

Web)	
Windows Malware Scan (Varredura de malware no Windows)	Para usuários buscando malware em sistemas Windows.
Mobile Device Scan (Varredura em dispositivo móvel)	Para usuários Apple Profile Manager, ADSI ou Good MDM.
Prepare for PCI DSS Audits (Preparação para auditorias PCI DSS)	Para usuários que estão se preparando para auditorias relacionadas à conformidade com PCI DSS.
Advanced Policy (Política avançada)	Para usuários que querem controle total da configuração de políticas.

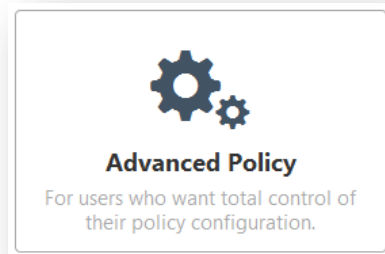
No decorrer do tempo, o assistente de políticas receberá assistentes adicionais para ajudar os clientes e os assistentes existentes a melhorarem ainda mais. A seguir, temos uma ideia geral do uso de um dos assistentes. Observe que cada assistente é diferente e que este é apenas um exemplo.

O primeiro passo em cada assistente solicita a definição do nome da política, da visibilidade da política (privada ou compartilhada) e de uma descrição. Por padrão, políticas do assistente permitirão a edição do relatório depois de uma varredura. Clique em “**Next**” (Avançar) para prosseguir para o próximo passo:

Essa política solicitará que você selecione se ela deverá ser usada para hosts internos ou externos, pois as opções dependerão da resposta. Clique em "**Next**" (Avançar) para ir para o último passo:

O passo final dá a opção de adicionar credenciais para aprimorar a varredura. Como observado, alguns passos de um assistente de política podem ser opcionais. Depois de criada, a política será salva com as configurações recomendadas. Você pode editar as opções do assistente ou qualquer outro aspecto da política a qualquer momento.

Criação de política avançada

Se não for desejado um assistente de política, a opção Advanced (Avançada) permite criar uma política da forma tradicional, com controle total sobre todas as opções desde o início.

Observe que existem quatro guias de configuração: **General Settings** (Configurações gerais), **Credentials** (Credenciais), **Plugins** e **Preferences** (Preferências). Na maioria dos ambientes, não é necessário modificar as configurações padrão, mas elas permitem um controle mais individualizado sobre o funcionamento do scanner Nessus. Essas guias são descritas a seguir.

General Settings (Configurações gerais)

A guia "**General Settings**" (Configurações gerais) permite nomear a política e configurar as operações de varredura. Há quatro itens de menu suspenso que controlam o comportamento do scanner:

A tela "**Basic**" (Básico) é usada para definir os aspectos da política em si:

Opção	Descrição
Name (Nome)	Define o nome a ser exibido na interface do usuário Nessus para identificar a política.
Visibility (Visibilidade)	Controla se a política é *compartilhada* (*shared*) com outros usuários ou mantida somente para uso *privado* (*private*). Somente usuários com status de administrador podem compartilhar políticas.
Description (Descrição)	Oferece uma breve descrição da política de varredura para resumir a finalidade geral (por exemplo: "Web Server scans without local checks or non HTTP services" (varreduras em servidores da Web sem verificações locais ou serviços não HTTP)).
Allow Post-Scan Report Editing (Permitir a edição do relatório pós-varredura)	Este recurso permite aos usuários excluir itens do relatório quando marcados. Ao realizar uma varredura para conformidade regulamentar ou outros tipos de auditoria, desmarque essa opção para mostrar que a varredura não foi adulterada.

O menu "**Port Scanning**" (Varredura de portas) controla as opções relacionadas à varredura de portas, incluindo intervalos de portas e métodos:

Opção	Descrição
Port Scan Range (Intervalo de varredura de porta)	Instrui o scanner a localizar um intervalo de portas específico. Aceita "default" (padrão), aproximadamente 4.790 portas comuns encontradas no arquivo `nessus-services`, "all" (todas), que varre 65.535 portas ou uma lista personalizada de portas especificada pelo usuário. Por exemplo: é possível usar "21,23,25,80,110" ou "1-1024,8080,9000-9200". A opção "1-65535" verificará todas as portas.

	Pode-se especificar também um intervalo de divisão específico para cada protocolo. Por exemplo: para verificar um intervalo de portas diferente para TCP e UDP na mesma política, é preciso especificar “T:1-1024,U:300-500”. Pode-se especificar também um conjunto de portas para varredura em ambos os protocolos, bem como intervalos individuais para cada protocolo separado ("1-1024,T:1024-65535,U:1025"). Se um único protocolo for verificado, selecione somente o scanner para aquela porta e especifique as portas normalmente.
Consider Unscanned Ports as Closed (Considerar portas não verificadas como fechadas)	Se uma porta não for examinada com um scanner de porta selecionado (por exemplo: fora do intervalo especificado), será considerada fechada pelo Nessus.
Nessus SNMP Scanner (Varredura Nessus SNMP)	Instrui o Nessus a examinar alvos para um serviço de SNMP. O Nessus detectará as configurações de SNMP correspondentes durante a varredura. Se as configurações forem feitas pelo usuário em “Preferences” (Preferências), o Nessus examinará totalmente o host remoto e produzirá resultados de auditoria mais detalhados. Por exemplo: muitas verificações do roteador Cisco determinam as vulnerabilidades presentes ao examinar a versão do string SNMP devolvido. Essas informações são necessárias para as auditorias.
Nessus UDP Scanner (Varredura Nessus UDP)	Esta opção usa o scanner de UDP integrado do Nessus para identificar as portas UDP abertas nos alvos. O UDP é um protocolo “sem estado”, ou seja, a comunicação não é feita com diálogos de reconhecimento. A comunicação por UDP nem sempre é confiável e, devido à natureza dos serviços UDP e dos dispositivos de rastreamento, nem sempre são detectáveis de maneira remota.
netstat portscanner (SSH) (Varredura de porta Netstat (SSH))	Esta opção usa o `netstat` para verificar se há portas abertas no computador local. Depende da disponibilidade do comando `netstat` por meio de uma conexão SSH com o alvo. Esta varredura se destina a sistemas do tipo Unix e requer credenciais de autenticação.
Ping the remote host (Ping para host remoto)	Esta opção permite que o Nessus envie um teste de ping aos hosts remotos em várias portas para determinar se estão ativos.
Netstat Portscanner (WMI) (Varredura de porta Netstat (WMI))	Esta opção usa o `netstat` para verificar se há portas abertas no computador local. Depende da disponibilidade do comando `netstat` por meio de uma conexão WMI com o alvo. Esta varredura se destina a sistemas do tipo Windows e requer credenciais de autenticação. A varredura por WMI usa o `netstat` para determinar portas abertas e, portanto, ignora todos os intervalos de portas especificados. Se um enumerador de portas (`netstat` ou SNMP) for executado, o intervalo de portas torna-se “all” (todas). No entanto, o Nessus manterá a opção “consider unscanned ports as closed” (considerar portas não verificadas como fechadas) se estiver selecionada.
Nessus TCP scanner (Varredura Nessus TCP)	Usa o scanner TCP integrado do Nessus para identificar portas TCP abertas nos alvos. Esse scanner é otimizado e conta com alguns recursos de ajuste automático.

	⚠ Em algumas plataformas (por exemplo: Windows e Mac OS X), a seleção do scanner fará com que o Nessus use o scanner SYN para evitar problemas graves de desempenho nativos desses sistemas operacionais.
Nessus SYN scanner (Varredura Nessus SYN)	Usa o scanner SYN integrado do Nessus para identificar portas TCP abertas nos alvos. As varreduras SYN são um método popular para realizar varreduras de portas e, geralmente, são consideradas um pouco menos invasivas do que as varreduras TCP. O scanner envia um pacote SYN à porta, aguarda a resposta SYN-ACK e determina o estado da porta de acordo com uma resposta ou a falta de resposta.

A opção "**Port Scan Range**" (Intervalo de varredura de portas) instrui o scanner a verificar um intervalo de portas específico. Os seguintes valores são permitidos:

Valor	Descrição
"default" (padrão)	Se a palavra-chave "**default**" (padrão) for usada, o Nessus examinará cerca de 4.790 portas comuns. A lista de portas pode ser encontrada no arquivo `nessus-services`.
"all" (todas)	Se a palavra-chave "**all**" (todas) for usada, o Nessus examinará todas as 65.535 portas.
Custom List (Lista personalizada)	Um intervalo personalizado de portas pode ser selecionado com o uso de uma lista delimitada por vírgulas de portas ou intervalos de portas. Por exemplo: é possível usar "21,23,25,80,110" ou "1-1024,8080,9000-9200". A opção "1-65535" verificará todas as portas. Pode-se especificar também um intervalo de divisão específico para cada protocolo. Por exemplo: para verificar um intervalo de portas diferente para TCP e UDP na mesma política, é preciso especificar "T:1-1024,U:300-500". Pode-se especificar também um conjunto de portas para varredura em ambos os protocolos, bem como intervalos individuais para cada protocolo separado ("1-1024,T:1024-65535,U:1025"). Se um único protocolo for verificado, selecione somente o scanner para aquela porta e especifique as portas normalmente.

O menu "**Performance**" (Desempenho) oferece opções que controlam o número de varreduras a ser iniciado. Essas opções podem ser as mais importantes ao configurar uma varredura, pois têm maior impacto sobre o tempo de varredura e a atividade da rede.

Opção	Descrição
Max Checks Per Host (Máx. verificações por Host)	Esta configuração limita o número máximo de verificações que um scanner Nessus realiza em um único host ao mesmo tempo.
Max Hosts Per Scan (Máx. Hosts por varredura)	Esta configuração limita o número máximo de hosts que um scanner Nessus pode verificar ao mesmo tempo.
Network Receive Timeout (seconds) (Tempo de espera por resposta da rede (segundos))	O valor padrão é cinco segundos. Esse é o tempo que o Nessus deve esperar por uma resposta do host, exceto se definido com outro valor por um plugin. Se a varredura for feita em uma conexão lenta, será preciso definir este valor com um número maior de segundos.
Max Simultaneous TCP Sessions Per Host (Máx. sessões TCP simultâneas	Esta configuração limita o número máximo de sessões TCP estabelecidas para um único host.

por Host)	⚠ Esta opção de congestionamento de TCP também controla o número de pacotes por segundo que o scanner SYN enviará (por exemplo: se esta opção estiver definida como 15, o scanner SYN enviará 1.500 pacotes por segundo, no máximo).
Max Simultaneous TCP Sessions Per Scan (Máx. sessões TCP simultâneas por varredura)	Esta configuração limita o número máximo de sessões TCP estabelecidas para toda a varredura, independentemente do número de hosts verificados. ⚠ Para os scanners Nessus instalados em computadores com Windows XP, Vista, 7 e 8, esse valor deve ser de no máximo 19 para se obter resultados precisos.
Reduce Parallel Connections on Congestion (Reduzir conexões paralelas em caso de congestionamento)	Permite que o Nessus detecte o envio de um grande número de pacotes e quando o pipe da rede atingir a capacidade máxima. Se forem detectados, o Nessus reduzirá a velocidade da varredura ao nível adequado para diminuir o congestionamento. Ao diminuir o congestionamento, o Nessus tentará reutilizar o espaço disponível no pipe da rede automaticamente.
Use Kernel Congestion Detection (Linux Only) (Utilizar detecção de congestionamento do Kernel (Somente Linux))	Permite que o Nessus monitore a CPU e outros mecanismos internos em caso de congestionamento e diminua o ritmo de maneira proporcional. O Nessus tentará usar sempre o máximo de recursos disponível. Este recurso está disponível apenas para os scanners Nessus instalados em Linux.

O menu “**Advanced**” (Avançado) define opções adicionais sobre como a varredura deve se comportar:

Opção	Descrição
Safe Checks (Verificações seguras)	A opção Safe Checks (Verificações seguras) desativa todos os plugins que podem afetar negativamente o host remoto.
Silent Dependencies (Dependências silencionsas)	Se esta opção for selecionada, a lista de dependências não será incluída no relatório. Se desejar incluir a lista de dependências no relatório, desmarque a caixa de seleção.
Log Scan Details to Server (Salvar detalhes da varredura no log do servidor)	Salva detalhes adicionais da varredura no registro do servidor Nessus (`nessusd.messages`), incluindo a ativação ou o encerramento do plugin ou se um plugin foi interrompido. O registro resultante pode ser usado para confirmar se determinados plugins foram usados e se os hosts foram examinados.
Stop Host Scan on Disconnect (Cessar a varredura do Host ao desconectar)	Se estiver selecionado, o Nessus cessará a varredura se detectar que o host parou de responder. Isso pode ocorrer se os usuários desligarem seus PCs durante uma varredura, se um host parar de responder após a negação de um plugin de serviço ou se o mecanismo de segurança (por exemplo: IDS) bloqueou o tráfego para um servidor. Se as varreduras continuarem nesses computadores, o tráfego desnecessário será enviado e atrasará a verificação.
Avoid Sequential Scans (Evitar varreduras consecutivas)	Normalmente, o Nessus verifica uma lista de endereços IP em sequência. Se a opção estiver marcada, o Nessus verificará a lista de hosts em ordem aleatória. Isto pode ser útil para ajudar a distribuir o tráfego de rede direcionado a uma sub-rede específica durante varreduras extensas.

	Antes de julho de 2013, essa opção funcionava com base em sub-rede. Desde então, o recurso foi aprimorado para usar todo o espaço IP alvo aleatoriamente.
Designate Hosts by their DNS Name (Designar Hosts pelo seu nome DNS)	Deve-se usar o nome do host em vez do endereço IP na impressão do relatório.

O intervalo especificado para uma varredura de portas será aplicado às varreduras TCP e UDP.

Credentials (Credenciais)

A guia “**Credentials”** (Credenciais) na imagem abaixo permite configurar o scanner Nessus para o uso de credenciais de autenticação durante a varredura. A definição de credenciais permite que o Nessus realize um número maior de verificações e gere resultados de varredura mais precisos.

O item de menu suspenso “**Windows credentials**” (Credenciais do Windows) tem configurações para fornecer ao Nessus informações, como o nome da conta SMB, senha e nome do domínio. O protocolo SMB (bloqueio de mensagens do servidor) é um protocolo de compartilhamento de arquivos que permite aos computadores compartilhar informações de forma transparente através da rede. Se as informações forem fornecidas, o Nessus poderá encontrar informações locais de um host Windows remoto. Por exemplo: o uso de credenciais permite que o Nessus determine se foram aplicados patches de segurança importantes. Não é necessário modificar outros parâmetros de SMB em relação às configurações padrão.

Quando diversas contas SMB forem configuradas, o Nessus tentará fazer o login com as credenciais fornecidas em sequência. Depois de ser autenticado com um conjunto de credenciais, o Nessus irá verificar as credenciais fornecidas subsequentes, mas só irá usá-las se os privilégios de administrador forem concedidos com o acesso do usuário pré-fornecido com as contas.

Algumas versões do Windows permitem criar uma nova conta e designá-la como um “administrator”. Essas contas nem sempre são adequadas para fazer varreduras com credenciais. A Tenable recomenda que a conta de administrador original, denominada “Administrator”, seja usada para varreduras com credenciais, para garantir que o acesso integral seja permitido. Em algumas versões do Windows, essa conta pode estar oculta. A conta de administrador real pode ser reexibida executando um prompt do DOS com privilégios de administrador e digitando o seguinte comando:

```
C:\> net user administrator /active:yes
```

Se uma conta SMB de manutenção for criada com privilégios limitados de administrador, o Nessus poderá realizar varreduras em diversos domínios de maneira fácil e segura.

A Tenable recomenda que os administradores de rede criem contas específicas de domínio para facilitar os testes. O Nessus conta com diversas verificações de segurança para Windows NT, 2000, Server 2003, XP, Vista, Windows 7, Windows 8 e Windows Server 2008, que serão mais precisas se uma conta de domínio for fornecida. Na maioria dos casos, o Nessus tentará aplicar diversas verificações caso uma conta não seja fornecida.

O serviço de registro remoto do Windows permite que computadores remotos com credenciais acessem o registro do computador a ser auditado. Se o serviço não estiver em execução, não será possível ler chaves e valores do registro, mesmo com credenciais completas. Para obter mais informações, consulte o artigo “Dynamic Remote Registry Auditing - Now you see it, now you don’t!” (Auditoria Dinâmica de Registro Remoto – Agora você vê, agora não!) no blog da Tenable. Esse serviço deve ser iniciado para que uma varredura com credenciais do Nessus audite integralmente um sistema usando credenciais.

Os usuários podem selecionar "**SSH settings**" (Configurações SSH) no menu suspenso e inserir credenciais para a varredura de sistemas Unix. As credenciais são usadas para obter informações locais de sistemas Unix remotos para auditoria de patches ou verificações de conformidade. Existe um campo para a inserção do nome de usuário do SSH da conta que realizará as verificações no sistema Unix de destino, juntamente com a senha ou chave pública do SSH e um par de chaves privadas. Existe também um campo para a inserção da frase-senha da chave SSH, se necessário.

> O Nessus permite o uso dos algoritmos de criptografia `blowfish-cbc`, `aes-cbc` e `aes-ctr`.

As varreduras com credenciais mais eficazes são aquelas em que as credenciais fornecidas têm privilégios de "root". Como muitos sites não permitem um login remoto como root, os usuários do Nessus podem chamar "**`su`**", "**`sudo`**", "**`su+sudo`**", "**`dzdo`**" ou "**pbrun**" com uma senha separada para uma conta que tenha sido configurada para ter privilégios de "**`su`**" ou "**`sudo`**". Além disso, o Nessus pode atribuir privilégios em dispositivos Cisco ao selecionar "**Cisco 'enable'**" (Cisco "habilitar").

O Nessus pode usar o acesso por chaves SSH para se autenticar em um servidor remoto. Se um arquivo SSH **`known_hosts`** estiver disponível e for fornecido com base na política de varredura, o Nessus tentará fazer o login apenas nos hosts desse arquivo. Além disso, a opção "Preferred SSH port" (Porta SSH preferencial) pode ser configurada para indicar ao Nessus que se conecte ao SSH se estiver funcionando em uma porta que não seja a porta 22.

O Nessus criptografa todas as senhas armazenadas nas políticas. No entanto, recomendamos o uso de chaves SSH para autenticação, em vez de senhas SSH. Isso ajuda a assegurar que o mesmo nome de usuário e senha usados para auditar os servidores SSH conhecidos não sejam usados para efetuar o login em um sistema que não esteja sob seu controle. Dessa forma, não é recomendável usar senhas SSH, a menos que seja absolutamente necessário.

A captura de tela a seguir mostra as opções SSH disponíveis. O menu suspenso “Elevate privileges with” (Elevar privilégios com) fornece os vários métodos de elevar os privilégios após serem autenticados.

Se outra conta for usada além de `root` para elevação de privilégios, pode ser especificada em “**Escalation account**” (Elevação de conta) com a opção “**Escalation password**” (Senha de elevação).

A “**Kerberos configuration**” (Configuração do Kerberos) permite especificar credenciais com o uso de chaves do Kerberos a partir de um sistema remoto:

Além disso, se um método seguro de varreduras credenciadas não estiver disponível, os usuários podem forçar o Nessus a executar varreduras por meio de protocolos sem segurança ao selecionar o item “**Cleartext protocol settings**” (Configurações de protocolo de texto simples) no menu suspenso. Os protocolos de texto simples disponíveis para esta opção são **telnet**, **rsh** e **rexec**. Além disso, há caixas de seleção para forçar o Nessus a executar varreduras em nível de patch em protocolos sem segurança:

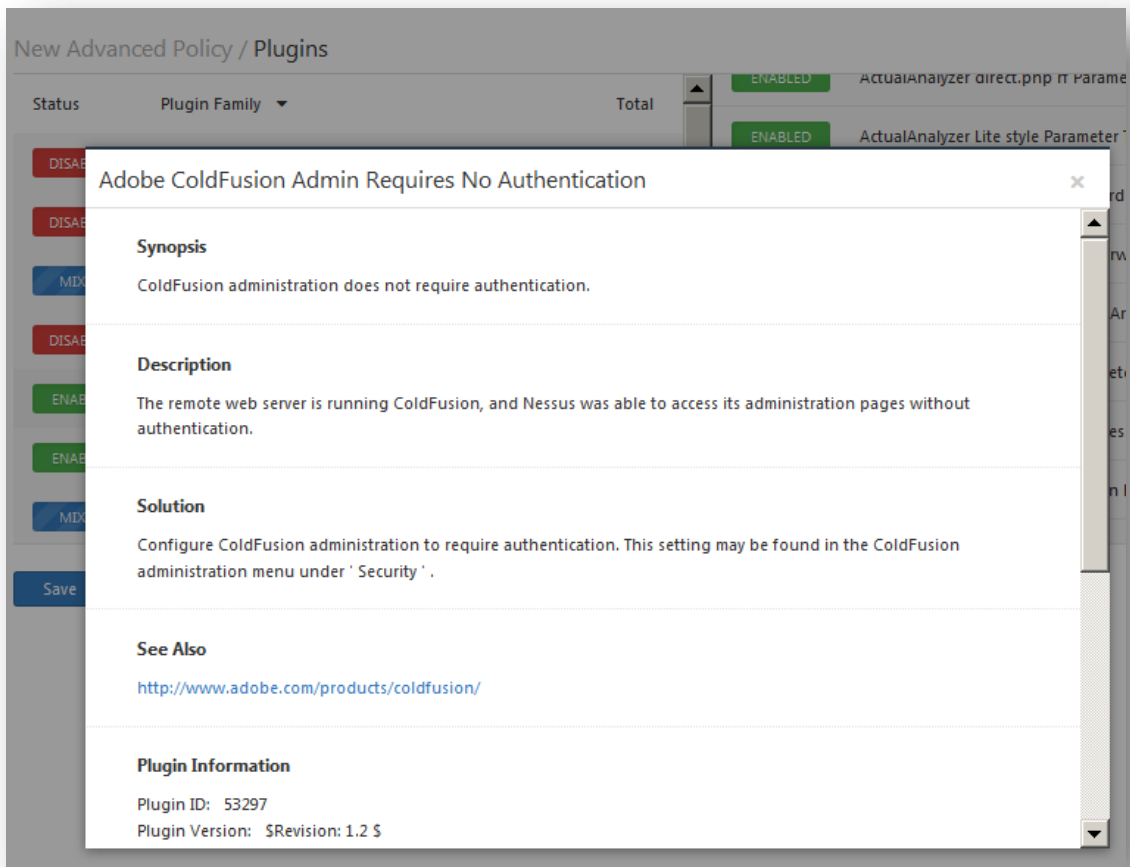
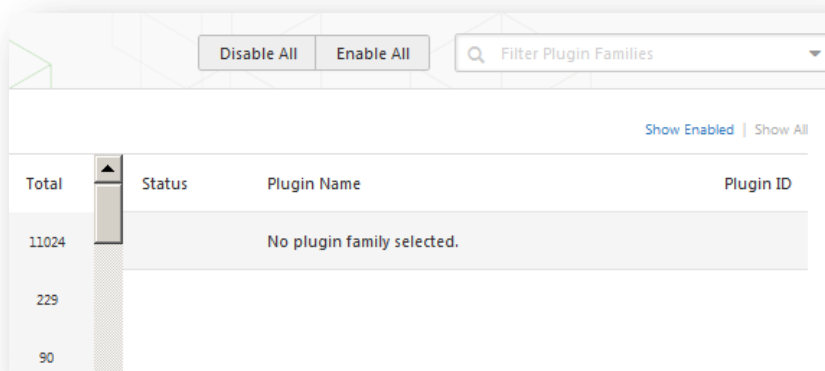
Normalmente, todas as senhas (e a própria política) são criptografadas. Se a política for salva em um arquivo `.nessus` e se o arquivo `.nessus` for posteriormente copiado em uma instalação do Nessus distinta, nenhuma senha da política poderá ser usada pelo segundo scanner Nessus, pois ele não será capaz de decodificá-la.

Não é recomendável usar credenciais em texto simples de qualquer tipo. Se as credenciais forem enviadas de maneira remota (por meio de uma varredura do Nessus, por exemplo), elas poderão ser interceptadas por qualquer pessoa com acesso à rede. Use mecanismos de autenticação criptografada sempre que possível.

Plugins

A guia “**Plugins**” permite que o usuário escolha verificações de segurança específicas por família de plugins ou verificações individuais.

Clicar na família de plugins permite ativar (verde) ou desativar (vermelho) toda a família. A seleção da família exibirá a lista de seus plugins. Plugins individuais podem ser ativados ou desativados para criar políticas de varredura específicas. Uma família com alguns plugins desabilitados ficará azul e exibirá “mixed” (misto) para indicar que apenas alguns dos plugins estão habilitados. Clicar na família de plugins carregará a lista completa de plugins e permitirá a seleção granular com base nas preferências de varredura.

A seleção de um plugin específico mostrará o resultado do plugin a ser exibido como em um relatório. O resumo e a descrição fornecerão mais detalhes sobre a vulnerabilidade a ser examinada. Rolar a tela para baixo no navegador também exibirá informações sobre soluções, referências adicionais se disponíveis, informações sobre riscos, informações sobre exploits e quaisquer referências cruzadas informativas ou de banco de dados de vulnerabilidades.

Na parte superior da página da família de plugins, é possível criar filtros para construir uma lista de plugins a serem incluídos na política, bem como desativar ou ativar todos os plugins. Os filtros permitem o controle granular sobre a seleção de plugins. Vários filtros podem ser definidos em uma única política.

Para filtrar plugins rapidamente com base no nome para localizar e ler sobre eles, digite na caixa de pesquisa. Isso filtrará os plugins dinamicamente. Além das pesquisas de texto, é possível digitar `id:10123` para filtrar rapidamente um plugin específico. Para criar um filtro, clique no botão “**Filter Options**” (Opções de filtro):

Cada filtro criado oferece várias opções para refinar a busca. Os critérios de filtragem podem se basear em “Any” (Qualquer), em que qualquer critério retornará correspondências, ou “All” (Todos), em que todos os critérios de filtragem devem estar presentes. Por exemplo, para pesquisar uma política que inclui apenas plugins que têm um exploit **ou** que pode ser explorado sem um exploit com script, é possível criar dois filtros e selecionar “Any” (Qualquer) como critério:

Para criar uma política que contenha plugins que correspondam a vários critérios, é possível selecionar “All” (Todos) e adicionar os filtros desejados. Por exemplo, a política a seguir deve incluir qualquer vulnerabilidade com uma correção publicada após 1 de janeiro de 2012 com um exploit público e CVSS Base Score superior a 5.0:

Para obter uma lista completa de critérios de filtragem, consulte a seção Filtros de relatórios deste documento.

Para usar filtros para a criação de políticas, recomenda-se começar desativando todos os plugins. Usando os filtros de plugins, selecione apenas os plugins que deseja incluir na política. Depois de concluído, selecione cada família de plugins e clique em “Enable Plugins”(Ativar plugins).

Ao criar e salvar uma política, todos os plugins selecionados inicialmente são armazenados. Quando novos plugins forem recebidos com a atualização de plugins, serão ativados automaticamente se a família à qual estiverem associados estiver ativa. Se a família estiver desativada ou parcialmente ativada, os novos plugins da família também serão desativados automaticamente.

A família “Denial of Service” (Negação de serviço) contém alguns plugins que podem causar falhas em uma rede corporativa caso a opção “Safe Checks” (Verificações seguras) não estiver ativa, mas contém algumas verificações úteis que não causam danos. A família “Denial of Service” (Negação de serviço) pode ser usada junto com “Safe Checks” (Verificações seguras) para garantir que nenhum plugin potencialmente nocivo seja executado. No entanto, recomenda-se que a família “Denial of Service” (Negação de serviço) não seja usada em uma rede de produção, a não ser que seja agendada durante uma janela de manutenção e com uma equipe pronta para responder em caso de problemas.

Preferences (Preferências)

A guia “**Preferences**” (Preferências) contém meios de controle individualizados para configuração de políticas de varredura. Selecione um item no menu suspenso para exibir itens de configuração adicionais para a categoria selecionada. Observe que essa é uma lista dinâmica de opções de configuração e depende da versão do Nessus, das políticas de auditoria e de outras funções às quais o scanner Nessus conectado tem acesso. Uma versão comercial do Nessus pode ter opções de configuração mais avançadas do que o Nessus Home. Esta lista também pode mudar à medida que os plugins são adicionados ou modificados.

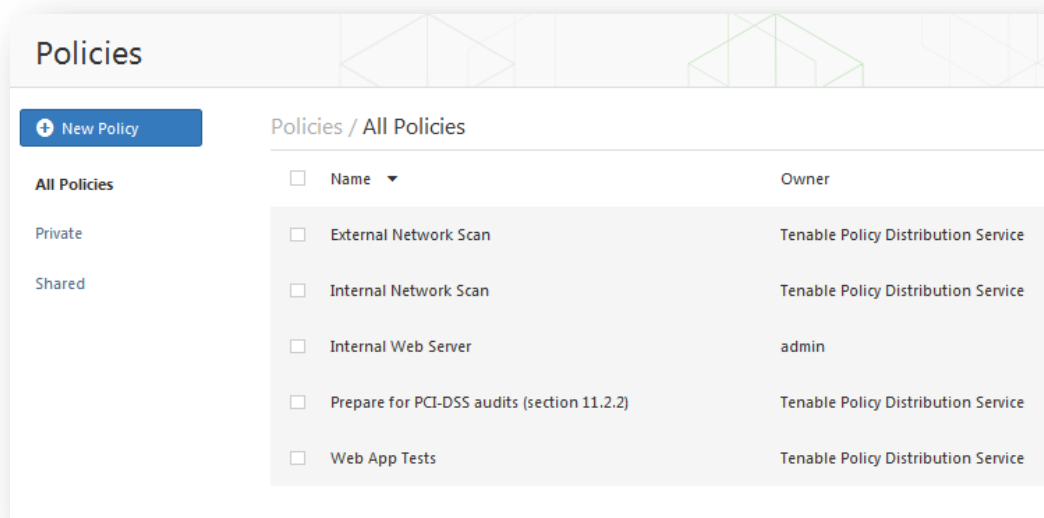
A tabela a seguir oferece uma descrição geral de todas as preferências. Para obter informações detalhadas com relação a cada item de preferência, consulte a seção Como verificar detalhes de preferências neste documento.

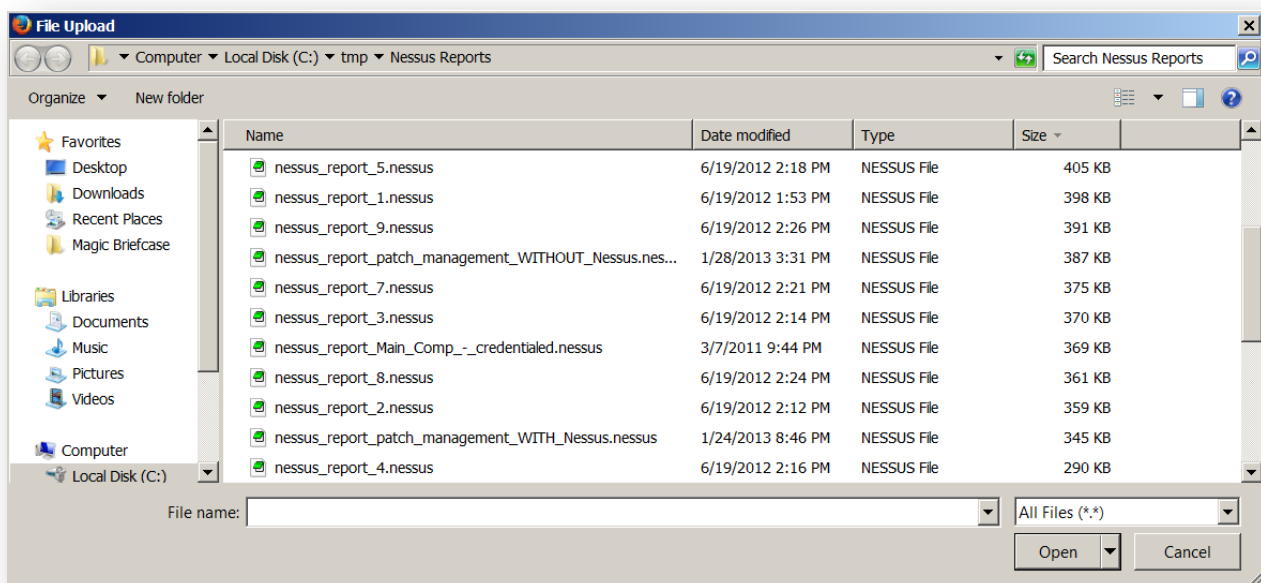
Menu Preference (Preferências)	Descrição
ADSI settings (Configurações de ADSI)	As Active Directory Service Interfaces (ADSI - Interfaces de serviço de diretório ativo) buscam informações do servidor de gerenciamento de dispositivos móveis (MDM) para dispositivos baseados em Android e iOS.
Apple Profile Manager API Settings (Configurações de API Apple Profile Manager)	Um recurso comercial que possibilita a enumeração e a varredura de vulnerabilidades de dispositivos Apple iOS (por exemplo, iPhone, iPad).
Cisco IOS Compliance Checks (Verificações de conformidade Cisco IOS)	Uma opção comercial que permite que um arquivo de política seja especificado para testar dispositivos Cisco IOS com relação a padrões de conformidade.
Database Compliance Checks (Verificações de conformidade de banco de dados)	Uma opção comercial que permite que um arquivo de política seja especificado para testar bancos de dados DB2, SQL Server, MySQL e Oracle com relação a padrões de conformidade.
Database Settings (Configurações de banco de dados)	Opções usadas para especificar o tipo de banco de dados a ser verificado, bem como as credenciais a serem usadas.
Do not scan fragile devices (Não verificar dispositivos frágeis)	Conjunto de opções que instrui o Nessus a **não** verificar dispositivos específicos devido ao risco de danificar o alvo.
Global variable settings (Configurações globais de variáveis)	Grande variedade de opções de configuração para o Nessus.
HTTP cookies import (Importação de cookies HTTP)	Para os testes de aplicativos da Web, esta preferência especifica um arquivo externo para a importação de cookies HTTP, de modo a permitir a autenticação do aplicativo.
HTTP login page (Página de login HTTP)	Definições relacionadas à página de login para testes de aplicativos da Web.
IBM iSeries Compliance Checks (Verificações de conformidade IBM iSeries)	Uma opção comercial que permite que um arquivo de política seja especificado para teste de sistemas IBM iSeries com relação a padrões de conformidade.
IBM iSeries Credentials (Credenciais para IBM iSeries)	Opção que especifica as credenciais para sistemas IBM iSeries.
ICCP/COTP TSAP Addressing Weakness (Endereçamento de vulnerabilidades ICCP/COTP TSAP)	Uma opção comercial relacionada aos testes Controle de supervisão e aquisição de dados (SCADA).
Login configurations (Configurações de login)	Local em que as credenciais são especificadas para teste de serviços HTTP, NNTP, FTP, POP e IMAP básicos.
Modbus/TCP Coil Access (Acesso Modbus/TCP Coil)	Uma opção comercial relacionada aos testes Controle de supervisão e aquisição de dados (SCADA).

Nessus SYN scanner (Scanner Nessus SYN)	Opções relacionadas ao scanner SYN integrado.
Nessus TCP scanner (Scanner Nessus TCP)	Opções relacionadas ao scanner TCP integrado.
News Server (NNTP) Information Disclosure (Divulgação de informações nos servidores de notícias (NNTP))	Um conjunto de opções que verifica a presença de vulnerabilidades de divulgação de informações nos servidores NNTP.
Oracle Settings (Configurações Oracle)	Opções relacionadas às instalações de banco de dados do Oracle.
PCI DSS compliance (Conformidade PCI DSS)	Uma opção comercial que instrui o Nessus a comparar os resultados de varredura com relação aos "PCI DSS standards" (padrões PCI DSS).
Patch Management: Red Hat Satellite Server Settings (Gerenciamento de patch: configurações de servidor satellite Red Hat)	Opções de integração do Nessus com o servidor de gerenciamento de patches Red Hat Satellite. Consulte o documento "Patch Management Integration" (Integração de Gerenciamento de Patches) para obter mais informações.
Patch Management: SCCM Server Settings (Gerenciamento de patch: configurações de servidor SCCM)	Opções de integração do Nessus com o servidor de gerenciamento de patches System Center Configuration Manager (SCCM). Consulte o documento "Patch Management Integration" (Integração de Gerenciamento de Patches) para obter mais informações.
Patch Management: VMware Go Server Settings (Gerenciamento de patch: configurações de servidor VMware Go)	Opções de integração do Nessus com o servidor de gerenciamento de patches VMware Go Server (Shavlik). Consulte o documento "Patch Management Integration" (Integração de Gerenciamento de Patches) para obter mais informações.
Patch Management: WSUS Server Settings (Gerenciamento de patch: configurações de servidor WSUS)	Opções de integração do Nessus com o servidor de gerenciamento de patches Windows Server Update Service (WSUS) (Serviço de atualização do Servidor Windows). Consulte o documento "Patch Management Integration" (Integração de Gerenciamento de Patches) para obter mais informações.
Ping the remote host (Ping para host remoto)	Opções que permitem controlar descobertas de rede com base no ping do Nessus.
Port scanner settings (Configurações de varredura de portas)	Duas opções que oferecem mais controle sobre a atividade de varredura de portas.
SMB Registry : Start the Registry Service during the scan (Registro SMB: iniciar o Serviço de Registro durante a varredura)	Instrui o Nessus a iniciar o serviço de registro SMB em hosts que não o possuem ativado.
SMB Scope (Alcance do SMB)	Instrui o Nessus a consultar os usuários do domínio em vez dos usuários locais.

SMB Use Domain SID to Enumerate Users (SMB: Usar SID de domínio para enumerar usuários)	Opção que permite especificar o intervalo de SID para pesquisas SMB de usuários do domínio.
SMB Use Host SID to Enumerate Local Users (SMB: Usar SID de host para enumerar usuários locais)	Opção que permite especificar o intervalo de SID para pesquisas SMB de usuários locais.
SMTP Settings (Configurações SMTP)	Opções de verificação de Simple Mail Transport Protocol (SMTP).
SNMP Settings (Configurações SNMP)	Informações de configuração e autenticação para Simple Network Management Protocol (SNMP).
Service Detection (Detecção do serviços)	Opções que permitem ao Nessus verificar os serviços baseados em SSL.
Unix Compliance Checks (Verificações de conformidade Unix)	Uma opção comercial que permite que um arquivo de política seja especificado para teste de sistemas Unix com relação a padrões de conformidade.
VMware SOAP API Settings (Configurações de VMware SOAP API)	Informações de configuração e autenticação para SOAP APIs da VMware.
Wake-on-LAN (Arranque remoto de LAN)	Instrui o Nessus a enviar pacotes Wake-on-LAN (WOL) antes de executar uma varredura.
Web Application Test Settings (Configurações de testes de aplicativos da Web)	Opções relacionadas a testes de aplicativos da Web.
Web mirroring (Espelhamento Web)	Detalhes de configuração que controlam o número de páginas da Web que o Nessus irá espelhar para analisar o conteúdo das vulnerabilidades.
Windows Compliance Checks (Verificações de conformidade Windows)	Uma opção comercial que permite que um arquivo de política seja especificado para teste de sistemas Windows com relação a padrões de conformidade.
Windows File Contents Compliance Checks (Verificações de conformidade de conteúdos de arquivos do Windows)	Uma opção comercial que permite que um arquivo de política seja especificado para teste de arquivos do sistema Windows com relação a padrões de conformidade.

Devido às atualizações de metadados do XML no Nessus 5, os dados de conformidade gerados com o Nessus 4 não estarão disponíveis no capítulo de verificações de conformidade dos relatórios exportados. No entanto, os dados de conformidade estarão disponíveis na interface do usuário Nessus.

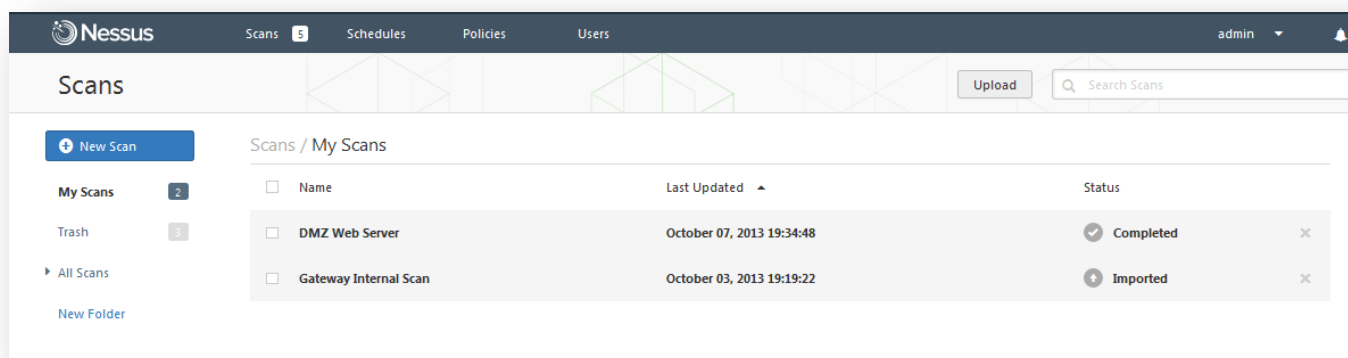
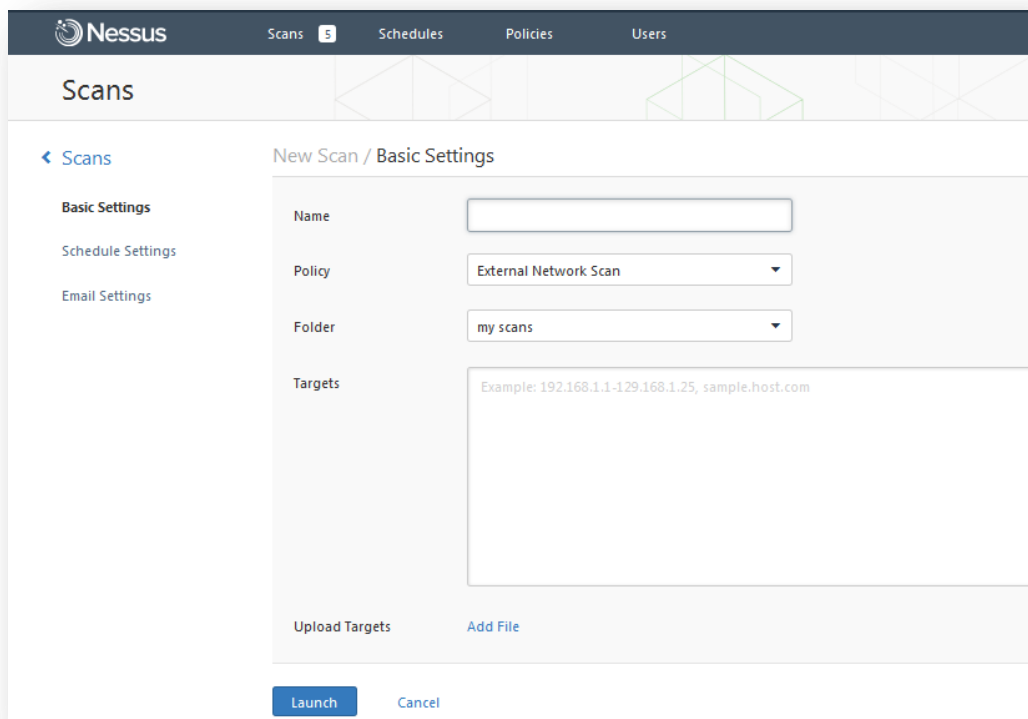
Para conveniência organizacional, o Nessus tem dois filtros predefinidos no lado esquerdo para políticas “Private” (Privadas) e “Shared” (Compartilhadas):

Importar, exportar e copiar políticas

O botão “**Upload**” (Fazer upload) na barra de menu Policies (Políticas) permite carregar no scanner políticas criadas anteriormente. Usando a caixa nativa do navegador de arquivos, selecione a política no sistema local e clique em “**Open**” (Abrir):

O botão “**Options**” (Opções) na barra de menus permite fazer o download de uma política selecionada do scanner para o sistema de arquivos local. A caixa de diálogo de download do navegador permite abrir a política em um programa externo (por exemplo, editor de texto) ou salvá-la em um diretório de sua preferência.

> As senhas e os arquivos `.audit` presentes em uma política não serão exportados.

Para criar uma política semelhante a uma política existente, mas com algumas modificações, selecione a política básica na lista e clique em “**Options**” (Opções) e, em seguida, em “**Copy Policy**” (Copiar política) na barra de menus. Isso criará uma cópia da política original, que pode ser editada para fazer todas as modificações necessárias. Isso permite criar políticas padrão com pequenas alterações necessárias para um determinado ambiente.

Criar, iniciar e programar uma varredura

Os usuários podem criar o próprio relatório por capítulos: Vulnerability Centric (Centrado em vulnerabilidades), Host Centric (Centrado no host), Compliance (Conformidade) ou Compliance Executive (Executivo de conformidade). O formato HTML ainda é o padrão. No entanto, se o Java estiver instalado no host do scanner, também será possível exportar relatórios em PDF. Com o uso de filtros de relatório e os recursos de exportação, os usuários podem criar relatórios dinâmicos à sua própria escolha em vez de selecioná-los em uma lista específica.

Os seguintes status de varredura estão disponíveis na tabela de listas de varredura

Status da varredura	Descrição
Completed (Concluída)	A varredura foi concluída.
Canceled (Cancelada)	O usuário interrompeu a varredura antes do final.
Aborted (Interrompida)	A varredura foi interrompida devido a uma lista de alvos inválida ou a um erro do servidor (por exemplo, reinicialização, falha)
Imported (Importada)	A varredura foi importada usando a funcionalidade de upload.

Esses status só se aplicam a novas varreduras. Varreduras antigas são consideradas "concluídas". Varreduras com o mesmo status podem ser listadas por meio das pastas virtuais no painel de navegação esquerdo.

Depois de criar ou selecionar uma política, é possível criar uma nova varredura clicando na opção "**Scans**" (Varreduras) na barra de menus na parte superior e, em seguida, clicando no botão "**+ New Scan**" (+ Nova varredura) à esquerda. A tela "**New Scan**" (Nova varredura) é exibida como no exemplo a seguir:

Na guia "**Basic Settings**" (Configurações básicas), há cinco campos para preencher o alvo da varredura:

- **Name (Nome)** – Define o nome que será exibido na interface do usuário Nessus para identificar a política.
- **Policy (Política)** – Selecione uma política já criada a ser usada pela varredura para definir os parâmetros que controlam o comportamento de varredura do servidor Nessus.
- **Folder (Pasta)** – A pasta da IU do Nessus para armazenar os resultados da varredura.
- **Scan Targets (Alvos de varredura)** – Os alvos podem ser inseridos com um endereço IP simples (por exemplo: 192.168.0.1), um intervalo de IPs (por exemplo: 192.168.0.1-192.168.0.255), uma sub-rede com a notação CIDR (por exemplo: 192.168.0.0/24) ou um host resolvível (por exemplo: www.nessus.org).
- **Upload Targets (Alvos de upload)** – É possível importar um arquivo de texto com uma lista de hosts clicando em "**Add File**" (Adicionar arquivo) e selecionando um arquivo na máquina local.

O arquivo de host deve ser formatado como texto ASCII, com um host por linha e sem espaços ou linhas extras. A codificação Unicode/UTF-8 não é reconhecida.

Exemplo de formatos de arquivos de host:

Hosts individuais:

192.168.0.100

192.168.0.101
192.168.0.102

Intervalo de hosts:

192.168.0.100-192.168.0.102

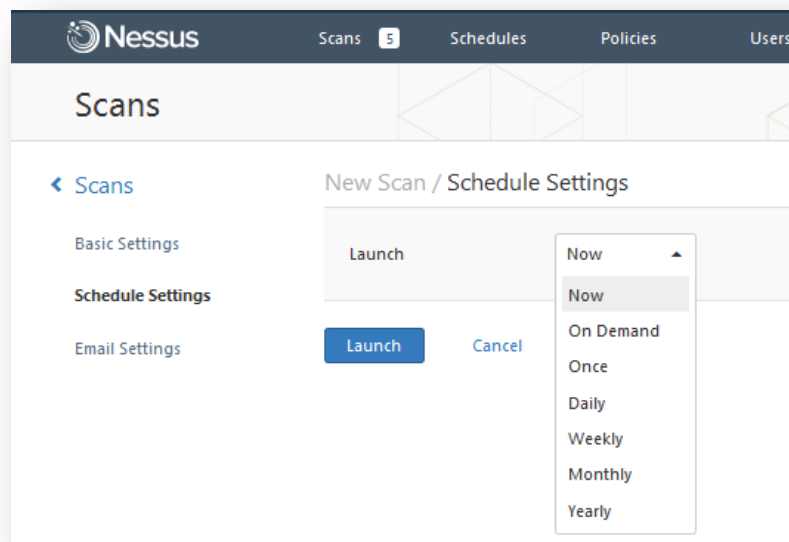
Bloco CIDR de hosts:

192.168.0.1/24

Servidores virtuais:

www.tenable.com[192.168.1.1]
www.nessus.org[192.168.1.1]
www.tenablesecurity.com[192.168.1.1]

Dependendo das configurações da varredura, como “**max hosts**” (máximo de hosts) ou “**max checks per host**” (máximo de verificações por host), isso poderá fazer com que hosts virtuais sejam limitados, pois o Nessus os vê com o mesmo endereço IP. Em hosts não Windows, os administradores do Nessus podem adicionar uma configuração personalizada avançada chamada **`multi_scan_same_host`** e defini-la como **`true`**. Isso permitirá que o scanner realize diversas varreduras no mesmo endereço IP. Observe que, no Windows, o driver PCAP não permite isso, independentemente da configuração do Nessus. Essa funcionalidade está disponível no Nessus 5.2.0 e posterior.

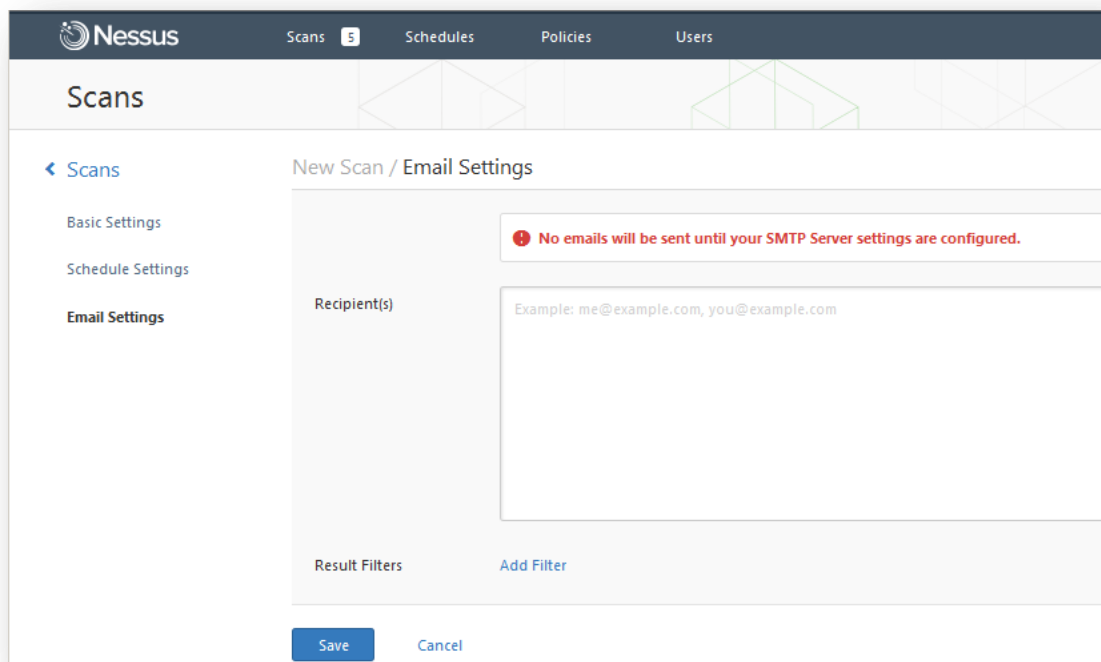
Na guia “**Schedule Settings**” (Configurações de agendamento) há um menu suspenso que controla quando a varredura será iniciada:

As opções de início são as seguintes:

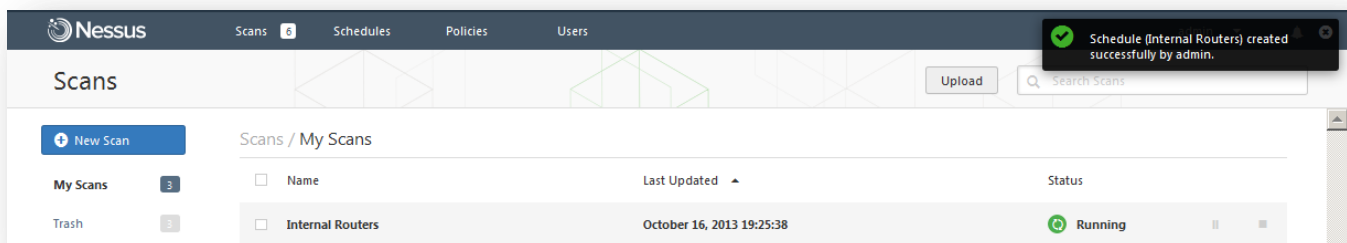
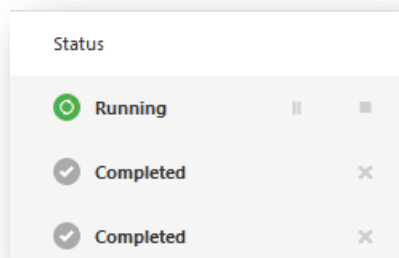
- **Now** (Agora) – Inicia a varredura imediatamente.
- **On Demand** (Sob demanda) – Crie a varredura como modelo para que ela possa ser iniciada manualmente em qualquer momento (esse recurso era tratado anteriormente na opção “Scan Template” (Modelo de varredura)).

- **Once** (Uma vez) – Agende a varredura em um horário específico.
- **Daily** (Diariamente) – Agende a varredura para que ocorra diariamente, em um horário específico ou em um intervalo, por até 20 dias.
- **Weekly** (Semanalmente) – Agende a varredura para que ocorra de forma recorrente, por horário e dia da semana, por até 20 semanas.
- **Monthly** (Mensalmente) – Agende a varredura para que ocorra todos os meses, por horário e dia ou semana do mês, por até 20 meses.
- **Yearly** (Anualmente) – Agende a varredura para que ocorra todos os anos, por horário e dia, por até 20 anos.

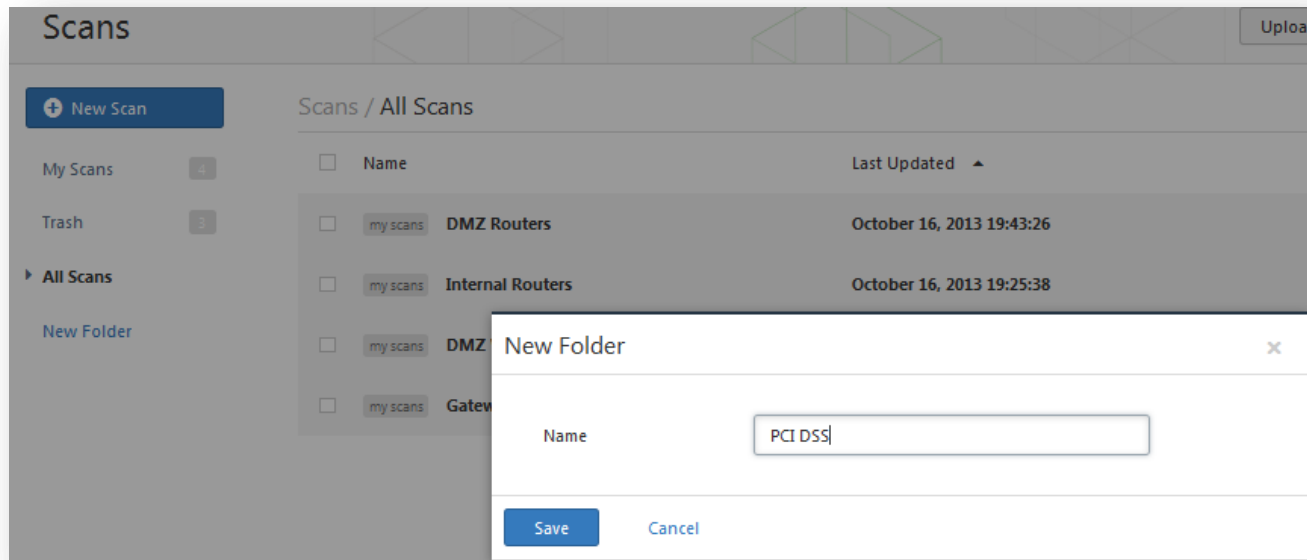
Abaixo está um exemplo de varredura agendada:

Quando uma varredura agendada é criada, ela pode ser acessada no menu "Schedules" (Agendamentos) na parte superior. Essa página permite gerenciar varreduras agendadas e atualizá-las conforme necessário:

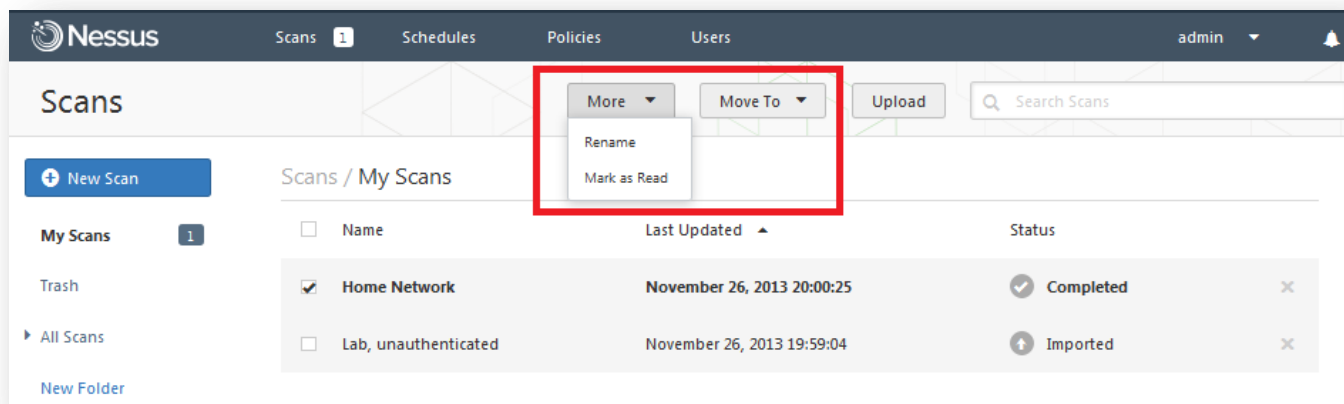
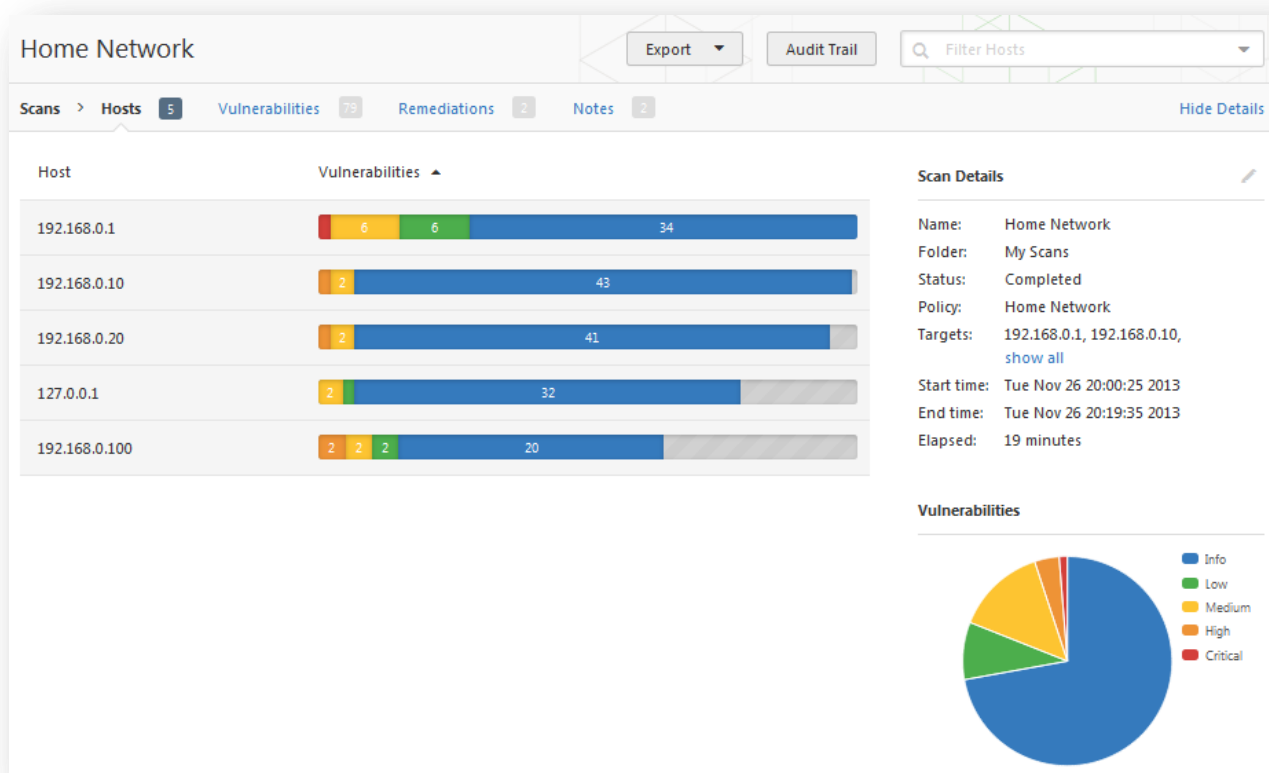
Na guia "**Email Settings**" (Configurações de e-mail), você pode configurar endereços de e-mail para os quais os resultados da varredura serão enviados quando ela for concluída.

A funcionalidade “**Email Scan Results**” (Enviar resultados da varredura por e-mail) requer que um administrador do Nessus defina as configurações de SMTP. Para obter mais informações sobre a definição de configurações de SMTP, consulte o “Nessus 5.2 Installation and Configuration Guide” (Guia de instalação e configuração do Nessus 5.2). Se você não definiu essas configurações, o Nessus avisará que elas precisam ser definidas para que a funcionalidade seja usada.

Depois de inserir as informações de varredura, clique em “**Save**” (Salvar). Depois do envio, a varredura iniciará imediatamente (se “**Now**” (Agora) foi selecionado) antes que a tela retorne à página geral de “**Scans**” (Varreduras). A barra de menus superior também atualizará o número no botão “**Scans**” (Varreduras) para indicar o total de varreduras presentes.

Depois que a varredura for iniciada, a lista “**Scans**” (Varreduras) exibirá uma lista de todas as varreduras em execução ou em pausa, além de informações básicas sobre cada varredura. Quando uma varredura está sendo executada, botões de pausar e parar são apresentados à esquerda para alterar o status:

Depois de selecionar uma varredura particular na lista usando a caixa de seleção à esquerda, os botões “**More**” (Mais) e “**Move To**” (Mover para) no canto superior direito permitirão realizar ações adicionais, incluindo a capacidade de renomear, manipular status de varreduras, marcar como lida ou movê-la para uma pasta diferente.

Procurar resultados de varreduras

As varreduras podem ser organizadas em pastas. À esquerda, há duas pastas padrão, My Scans (Minhas varreduras) e Trash (Lixeira). Por padrão, todas as varreduras novas serão exibidas na pasta virtual **My Scans** (Minhas varreduras). O local padrão para novas varreduras pode ser alterado usando pastas adicionais que podem ser criadas com a opção “**New Folder**” (Nova pasta), mostrada abaixo:

As pastas também podem ser gerenciadas usando o menu “**User Profile**” (Perfil do usuário) -> “**Folders**” (Pastas).

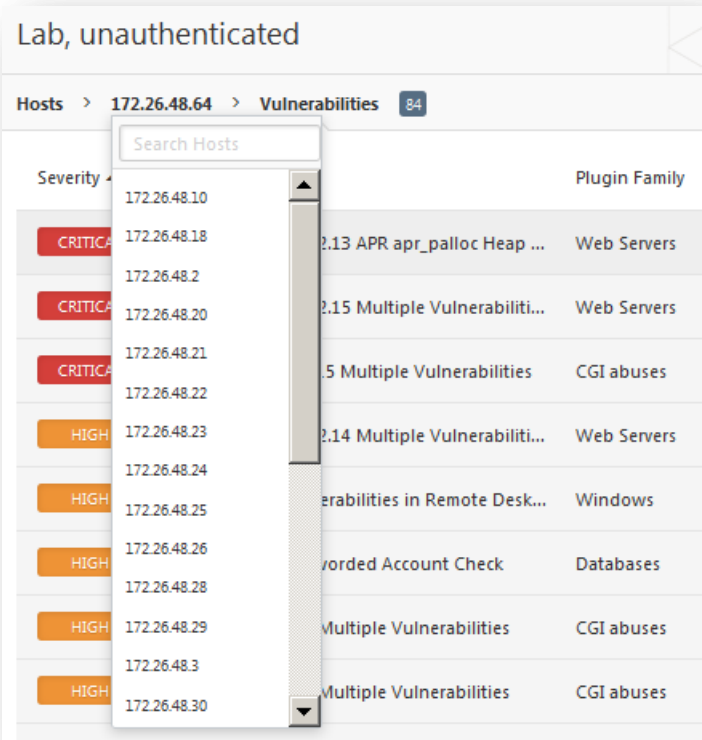
Varreduras na pasta “Trash” (Lixeira) serão excluídas automaticamente depois de 30 dias. Elas podem ser excluídas a qualquer momento apagando-as individualmente ou selecionando “**Empty Trash**” (Esvaziar lixeira) na parte superior.

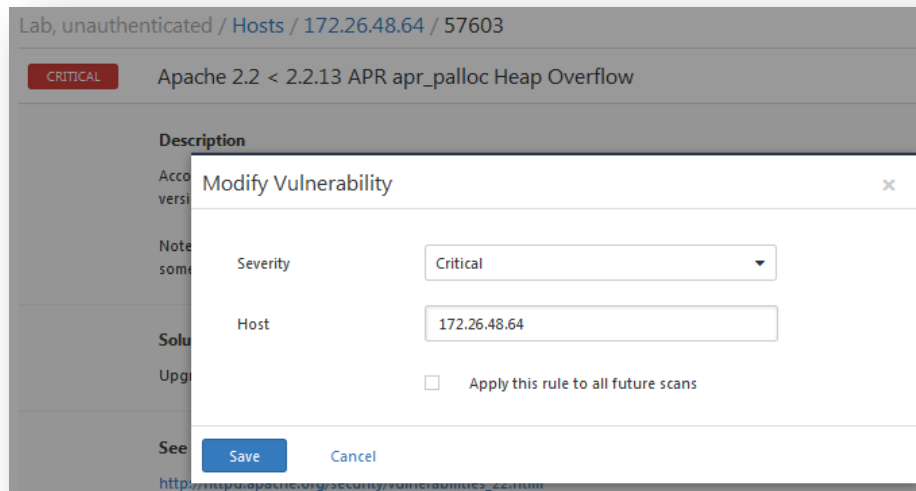
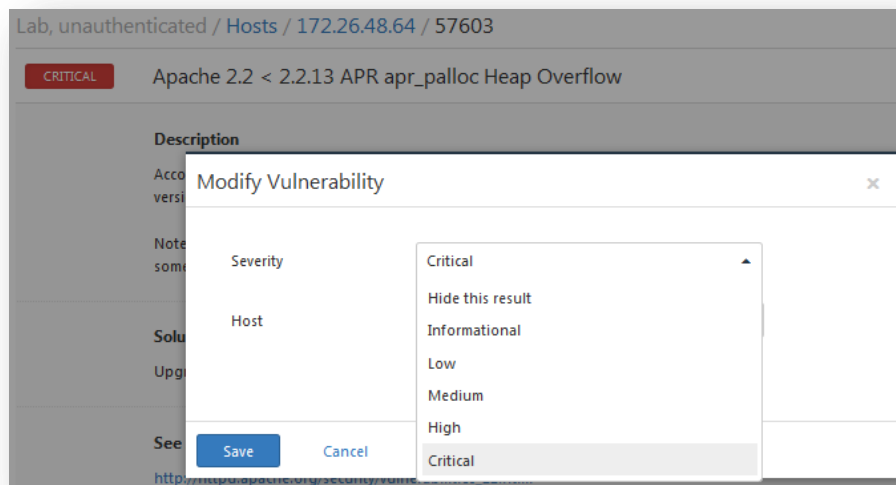
Para mover os resultados de varreduras entre pastas, selecione a varredura marcando a caixa à esquerda. Depois de marcada, menus suspensos adicionais serão exibidos na parte superior. Um deles fornece opções “More” (Mais), incluindo renomear e marcar uma varredura como lida ou não lida. O segundo permite mover a varredura para a pasta desejada.

Para procurar os resultados de uma varredura, clique em um relatório da lista. Isso permite exibir os resultados ao navegar pelos resultados de vulnerabilidades ou hosts, exibir portas e informações de vulnerabilidades específicas. A exibição/guia padrão é por resumo de host, que exibe uma lista de hosts com um resumo de vulnerabilidades codificado por cores para cada host:

Se ocorrer algum erro durante a varredura, haverá uma notação na parte superior dos resultados:

Network interface not supported
The network interface '\Device\{F3957D14-D708-454D-93A7-C7DFF8F076F6}' does not support packet forgery. This prevents Nessus from determining whether some of the target hosts are alive and from performing a full port scan against them. You may partially work around this problem by editing your scan settings to disable 'Ping' (Uncheck General->Ping host) and by providing Nessus with credentials to the remote host to prevent a port scan from taking place, however it would be preferable to scan over a different network interface.

Clicar em "Hide Details" (Ocultar detalhes) na parte superior direita, suprimirá os Scan Details (Detalhes de varredura) para mostrar mais do resumo do host.

Na exibição de resumo de "Hosts", cada resumo conterá detalhes sobre a vulnerabilidade ou resultados informativos, assim como **Host Details** (Detalhes do host) que fornecem informações gerais sobre o host varrido. Se “**Allow Post-Scan Report Editing**” (Permitir a edição do relatório pós-varredura) foi selecionado nas políticas de varredura, um host pode ser excluído dos resultados da varredura selecionando o ícone de lixeira à direita de **Host Details** (Detalhes do host).

Para alterar rapidamente entre os hosts, clique no host através do fluxo de navegação na parte superior para exibir um menu suspenso de outros hosts. Se houver diversos hosts, uma caixa de busca estará disponível para obter a localização rápida de hosts:

Clicar em uma vulnerabilidade através das guias Hosts ou Vulnerabilities (Vulnerabilidades) exibirá informações de vulnerabilidade, incluindo uma descrição, uma solução, referências e qualquer saída de plugin disponível. **Plugin Details** (Detalhes do plugin) serão exibidos à direita, fornecendo informações adicionais sobre o plugin e sobre a vulnerabilidade associada. Nessa tela, o ícone de caneta à direita de **Plugin Details** (Detalhes do plugin) poderá ser usado para modificar a vulnerabilidade exibida:

Clicar no ícone de caneta fará com que uma caixa de diálogo, como mostrado abaixo, seja exibida:

O menu suspenso de gravidade permitirá que você reclassifique o nível de gravidade da vulnerabilidade em questão, além de poder ocultá-lo no relatório:

Após a alteração ser realizada, clicar em "**Save**" (Salvar) salvará a alteração e a aplicará à vulnerabilidade em questão. Além disso, a modificação pode ser aplicada a todos os relatórios futuros clicando na opção. Realizar essa ação exibirá uma caixa de diálogo que permite que você defina a data de expiração da regra de modificação:

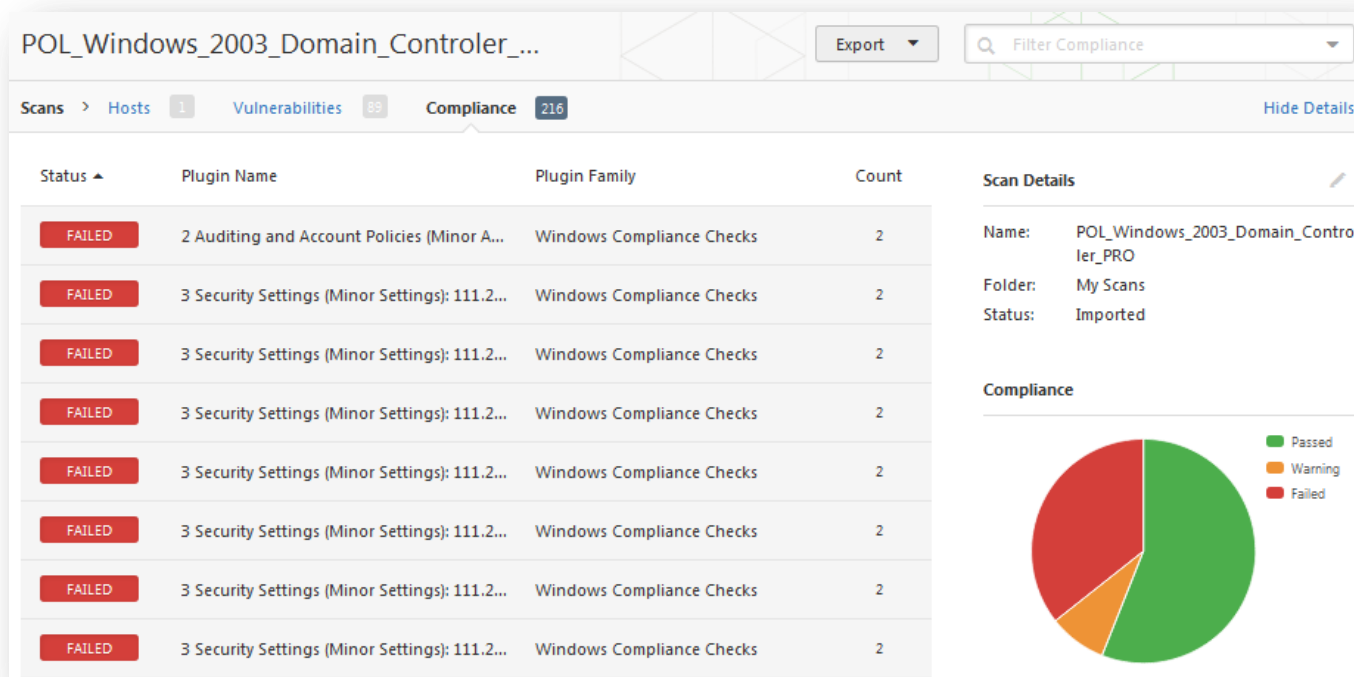
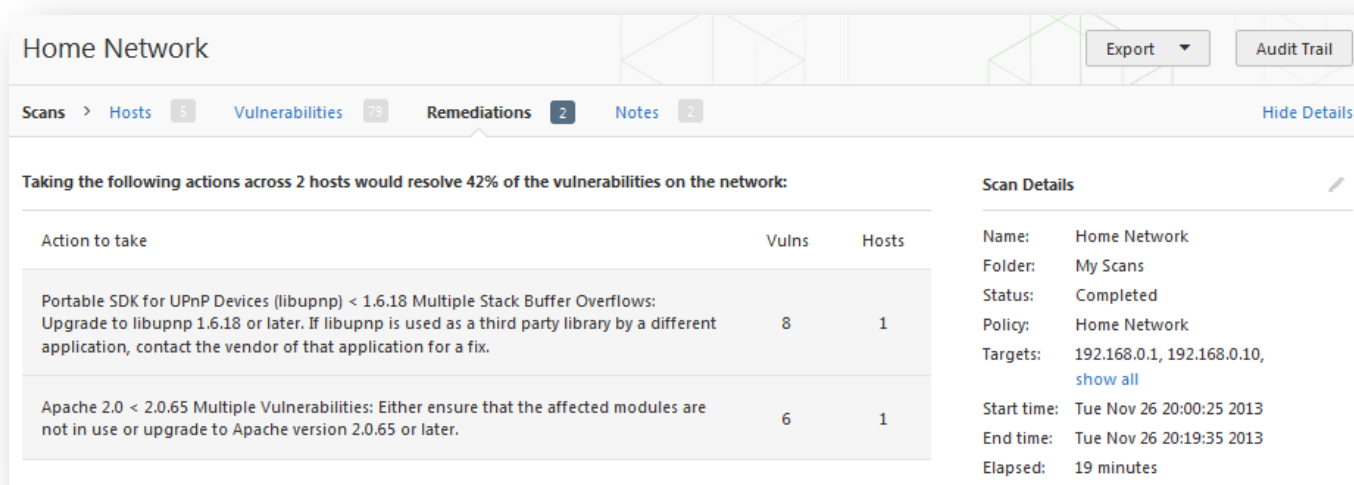
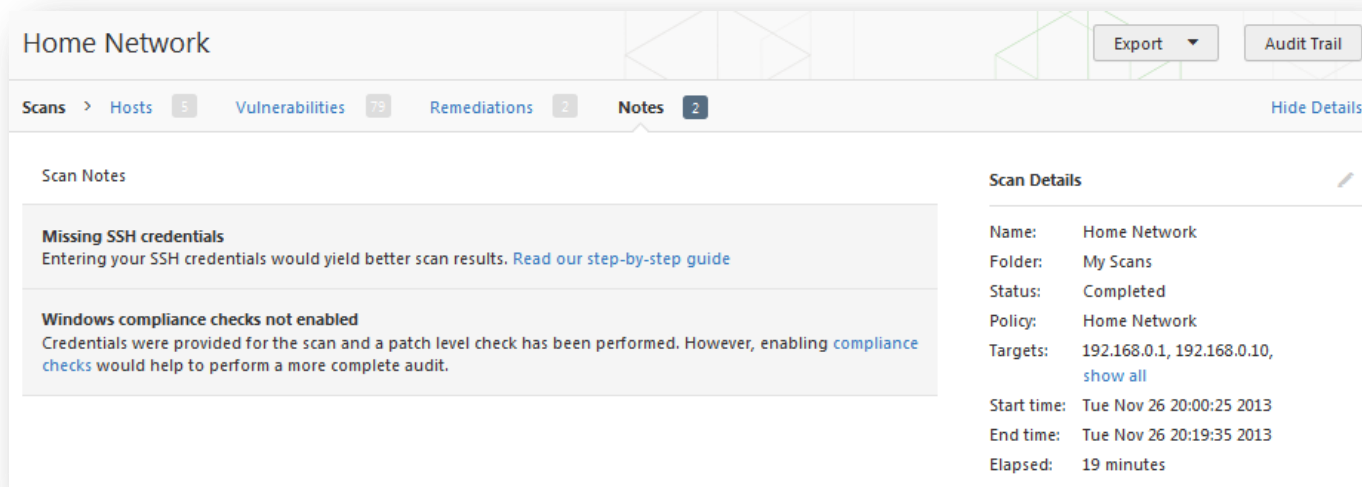
Uma data de expiração pode ser selecionada usando o calendário. Nessa data, a regra de modificação especificada não será mais aplicada àquele resultado.

Observe que as regras globais para risco/gravidade do plugin de reformulação podem ser estabelecidas na área "**User Profile**" (Perfil do usuário) -> "**Plugin Rules**" (Regras do plugin) no Nessus.

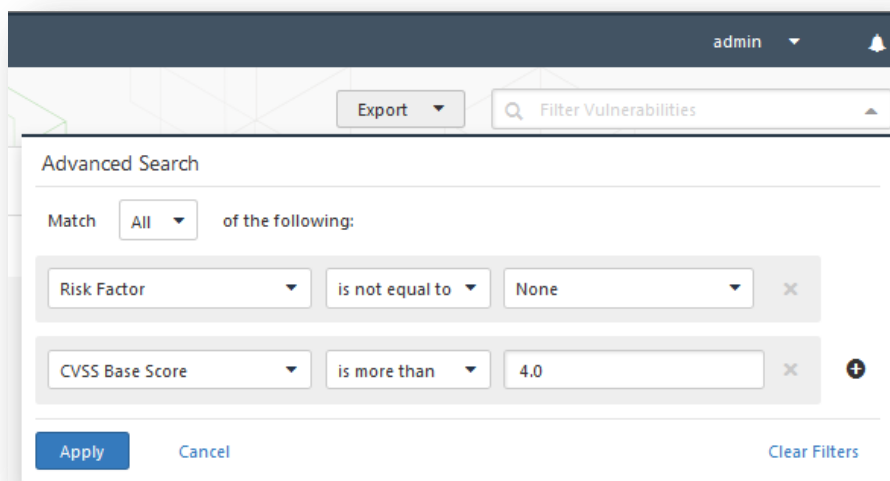
As classificações de gravidade são derivadas da respectiva pontuação CVSS, em que 0 é "Info", inferior a 4 é "Low" (baixo), inferior a 7 é "Medium" (médio), inferior a 10 é "High" (alto) e uma pontuação CVSS igual a 10 será indicada como "Critical" (grave).

Selecionar a guia "**Vulnerabilities**" (Vulnerabilidades) na parte superior alternará a exibição de vulnerabilidade. Isso classificará os resultados por vulnerabilidades, em vez de por hosts, e incluirá o número de hosts afetados à direita. Selecionar uma vulnerabilidade fornecerá as mesmas informações que antes, mas incluirá também uma lista dos hosts afetados na parte inferior.

Clicar em um host afetado na parte inferior carregará a exibição baseada em hosts das vulnerabilidades.

Se uma varredura for iniciada, usando uma compliance policy (política de conformidade), os resultados serão apresentados separados na parte superior chamada “**Compliance**” (Conformidade):

Além das guias **Hosts** e **Vulnerabilities** (Vulnerabilidades), o Nessus oferece mais duas guias adicionais. A primeira é a guia **Remediations** (Correções), que fornece informações resumidas para corrigir os problemas principais que foram detectados. Este conselho visa disponibilizar a atenuação mais eficaz, o que reduzirá significativamente o número de vulnerabilidades:

A segunda guia é chamada Notes (Observações) e oferece conselhos de como aprimorar os resultados de varredura:

Filtros de relatórios

O Nessus oferece um sistema de filtros flexível para auxiliar na exibição de resultados específicos do relatório. Os filtros podem ser usados para exibir os resultados de acordo com qualquer aspecto dos resultados de vulnerabilidades. Quando vários filtros forem usados, será possível criar exibições mais detalhadas e personalizadas dos relatórios.

O primeiro tipo de filtro é uma string de texto inserida na caixa "**Filter Vulnerabilities**" (Filtrar vulnerabilidades) na parte superior direita. Assim que você digitar, o Nessus iniciará imediatamente a filtragem dos resultados com base no texto e nas correspondências dos títulos dos resultados. O segundo tipo de filtro é mais abrangente e permite a especificação de mais detalhes. Para criar esse tipo de filtro, clique na seta para baixo à direita da caixa "**Filter Vulnerabilities**" (Filtrar vulnerabilidades). Os filtros podem ser criados a partir de qualquer guia de relatório. Vários filtros podem ser criados com lógica que permite a filtragem complexa. Um filtro é criado ao selecionar o atributo de plugin, argumento de filtro e um valor de filtragem: Ao selecionar diversos filtros, especifique a palavra-chave "Any" (Qualquer) ou "All" (Todos) adequadamente. Se "All" (Todos) for selecionado, todos os resultados correspondentes aos filtros **all** (todos) serão exibidos:

Depois de ter sido definido, o filtro poderá ser removido individualmente ao clicar no ✖ à direita. Além disso, todos os filtros podem ser removidos ao mesmo tempo ao selecionar "**Clear Filters**" (Limpar filtros). Os filtros de relatório aceitam uma grande variedade de critérios para controle granular dos resultados:

Opção	Descrição
Plugin ID (ID do plugin)	Filtra os resultados se a opção de Plugin ID (ID do plugin) for "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: 42111).
Plugin Description (Descrição do plugin)	Filtra os resultados se a opção de Plugin Description (Descrição do plugin) for "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "remote").
Plugin Name (Nome do plugin)	Filtra os resultados se a opção de Plugin Name (Nome do plugin) for "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "windows").
Plugin Family (Família de plugins)	Filtra os resultados se a opção de Plugin Name (Nome do plugin) for "*is equal to*" (igual a) ou "*is not equal to*" (diferente) para as famílias de plugin do Nessus designadas. As correspondências possíveis estão disponíveis no menu suspenso.
Plugin Output (Saída de plugin)	Filtra os resultados se a opção de Plugin Description (Descrição do plugin) for "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "PHP").
Plugin Type (Tipo de plugin)	Filtra os resultados se a opção de Plugin Type (Tipo de plugin) for "*is equal to*" (igual a) ou "*is not equal to*" (diferente) para um dos dois tipos de plugins: local ou remoto.
Solution (Solução)	Filtra os resultados se a opção de Solution (Solução) de plugin for "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "upgrade").
Synopsis (Sinopse)	Filtra os resultados se a opção de Solution (Solução) for "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "PHP").
Hostname (Nome do host)	Filtra os resultados se a opção de host for "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "192.168" ou "lab").
Port (Porta)	Filtra os resultados se a opção de porta for "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "80").
Protocol (Protocolo)	Filtra os resultados se a opção de protocolo for "*is equal to*" (igual a) ou "*is not equal to*" (diferente) para uma determinada string (por exemplo: "http").
CPE	Filtra os resultados se a opção de Common Platform Enumeration (CPE) (Enumeração de Plataforma Comum) for "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "solaris").
CVSS Base Score (Pontuação CVSS Base)	Filtra os resultados se a opção de CVSS Base Score (Pontuação CVSS Base) for "*is less than*" (inferior a), "*is more than*" (superior a), "*is equal to*" (igual a), "*is not equal to*"

	(diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "5"). Este filtro pode ser usado para selecionar o nível de risco. As classificações de gravidade são derivadas da respectiva pontuação CVSS, em que 0 é "Info", inferior a 4 é "Low" (baixo), inferior a 7 é "Medium" (médio), inferior a 10 é "High" (alto) e uma pontuação CVSS igual a 10 será indicada como "Critical" (grave).
CVSS Temporal Score (Pontuação CVSS Temporal)	Filtra os resultados se a opção de CVSS Temporal Score (Pontuação CVSS Temporal) for "*is less than*" (menor que), "*is more than*" (maior que), "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "3.3").
CVSS Temporal Vector (Vetor CVSS Temporal)	Filtra os resultados se a opção de CVSS Temporal Vector (Vetor CVSS Temporal) for "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "E:F").
CVSS Vector (Vetor CVSS)	Filtra os resultados se a opção de CVSS vector (Vetor CVSS) for "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "AV:N").
Vulnerability Publication Date (Data de publicação da vulnerabilidade)	Filtra os resultados com base na data de publicação da vulnerabilidade "*earlier than*" (inferior a), "*later than*" (superior a), "*on*" (em), "*not on*" (não em), "*contains*" (contém) ou "*does not contain*" (não contém) para uma string (por exemplo: "01/01/2012"). Observação: pressionar o botão próximo à data abrirá a interface do calendário para facilitar a escolha da data.
Patch Publication Date (Data de publicação do patch)	Filtra os resultados com base na data de publicação do patch com a opção "*is less than*" (menor que), "*is more than*" (maior que), "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma string (por exemplo: "12/01/2011").
Plugin Publication Date (Data de publicação do plugin)	Filtra os resultados com base na data de publicação do plugin do Nessus com a opção "*is less than*" (menor que), "*is more than*" (maior que), "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma string (por exemplo: "06/03/2011").
Plugin Modification Date (Data de modificação do plugin)	Filtra os resultados com base na data de modificação do plugin do Nessus com a opção "*is less than*" (menor que), "*is more than*" (maior que), "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma string (por exemplo: "02/14/2010").
CVE	Filtra os resultados se a opção de CVSS reference (referência CVSS) for "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "2011-0123").
Bugtraq ID	Filtra os resultados se a opção de Bugtraq ID (ID de Bugtraq) for "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "51300").

CERT Advisory ID (ID de aviso CERT)	Filtra os resultados se a opção de CERT Advisory ID (ID de aviso CERT) (também chamado de Technical Cyber Security Alert – Alerta Técnico de Segurança Cibernética) for "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "TA12-010A").
OSVDB ID (ID de OSVDB)	Filtra os resultados se a ID de Open Source Vulnerability Database (OSVDB) for "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "78300").
Secunia ID (ID de Secunia)	Filtra os resultados se a opção de Secunia ID (ID de Secunia) for "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "47650").
Exploit Database ID (ID do banco de dados de Exploit)	Filtra os resultados se a referência de Exploit Database ID (EBD-ID) (ID do banco de dados de Exploit) for "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "18380").
Metasploit Name (Nome do metasploit)	Filtra os resultados se a opção de Metasploit name (Nome do metasploit) for "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "xslt_password_reset").
Exploit Hub (Concentração de exploit)	Filtra os resultados se o exploit da ExploitHub (Concentração de exploit) for "*true*" (verdadeiro) ou "*false*" (falso).
IAVA	Filtra os resultados se a referência de IAVA for "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: 2012-A-0008).
IAVB	Filtra os resultados se a referência de IAVB for "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: 2012-A-0008).
IAVT	Filtra os resultados se a referência de IAVT for "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: 2012-A-0008).
See Also (Ver também)	Filtra os resultados se a referência "see also" (ver também) de plugins do Nessus for "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "seclists.org").
Exploits Available (Exploits disponíveis)	Filtra os resultados se a vulnerabilidade tiver uma exploração pública conhecida.
Exploitability Ease (Facilidade de exploração)	Filtra os resultados se a opção de facilidade de exploração for "*is equal to*" (igual a) ou "*is not equal to*" (diferente) para os seguintes valores: *Exploits are available*" (exploits disponíveis), "*No exploit is required*" (não requer exploits) ou "*No known exploits are available*" (nenhum exploit conhecido disponível).
Metasploit Exploit Framework (Quadro Metasploit Exploit)	Filtra os resultados com base na presença de uma vulnerabilidade no Metasploit Exploit Framework "*is equal to*" (igual a) ou "*is not equal to*" (diferente) verdadeiro ou falso.
CANVAS Exploit Framework	Filtra os resultados com base na presença de um exploit no CANVAS Exploit Framework "*is equal to*" (igual a) ou "*is not equal to*" (diferente) verdadeiro ou falso.

CANVAS Package (Pack CANVAS)	Filtra os resultados com base em a qual pacote do CANVAS Exploit Framework o exploit existe. As opções incluem CANVAS, D2ExploitPack ou White_Phosphorus.
CORE Exploit Framework	Filtra os resultados com base na presença de um exploit no CORE Exploit Framework "*is equal to*" (igual a) ou "*is not equal to*" (diferente) verdadeiro ou falso.
Elliot Exploit Framework	Filtra os resultados com base na presença de um exploit no Elliot Exploit Framework "*is equal to*" (igual a) ou "*is not equal to*" (diferente) verdadeiro ou falso.
Elliot Exploit Name	Filtra os resultados se o exploit Elliot for "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "Typo3 FD").
ExploitHub	Filtra os resultados com base na presença de um exploit no site ExploitHub "*is equal to*" (igual a) ou "*is not equal to*" (diferente) verdadeiro ou falso.

Quando um filtro é usado, é possível delimitar a string ou o valor numérico por vírgulas para filtrar com base em várias strings. Por exemplo: para filtrar os resultados de maneira a exibir apenas os servidores da Web, é preciso criar um filtro "Ports", selecionar "is equal to" (igual a) e inserir "80,443,8000,8080". Isto exibirá os resultados associados a essas quatro portas.

Os critérios de filtragem não distinguem maiúsculas e minúsculas.

Se uma opção de filtro não estiver disponível, significa que o relatório não contém nenhuma opção que corresponde aos critérios. Por exemplo: se "Microsoft Bulletin" não estiver na listagem de filtros, nenhuma vulnerabilidade referente a um boletim da Microsoft foi encontrada.

Assim que um filtro for criado, os resultados da varredura serão atualizados para refletir os novos critérios de filtragem após selecionar "**Apply**" (Aplicar). A seta pra baixo na caixa "**Filter Vulnerabilities**" (Filtrar vulnerabilidades) alterará para uma representação numérica de quantos filtros estão aplicados atualmente.

Depois que os resultados forem filtrados para gerar o conjunto de dados desejado, clique em "**Export Results**" (Exportar resultados) para exportar apenas os resultados filtrados. Para receber um relatório com todos os resultados, remova todos os filtros e use o recurso de exportação.

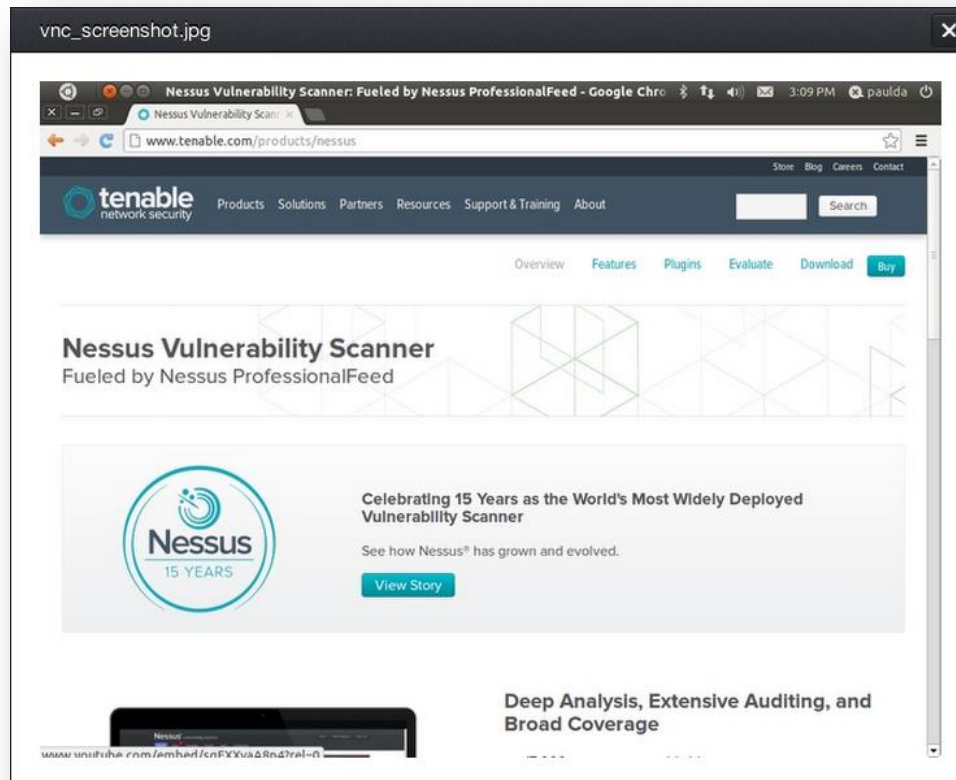
Os resultados de varredura do Nessus fornecem uma lista concisa dos plugins detectados com problema no host. No entanto, às vezes é necessário saber por que um plugin **não** enviou resultados. A funcionalidade "**Audit Trail**" (Trilha de auditoria) fornecerá essas informações. Comece clicando em "Audit Trail" (Trilha de auditoria) no canto superior direito:

Isso abrirá a caixa de diálogo Audit Trail (Trilha de auditoria). Digite a ID do plugin do qual deseja obter mais informações. Clique no botão “**Submit**” (Enviar) para exibir uma série ou lista de hosts relativos à consulta. Opcionalmente, é possível fornecer um IP do host para a consulta inicial para limitar os resultados de um destino de interesse. Quando o(s) host(s) for(em) exibido(s), clique em um host para mostrar informações sobre a causa da falha do plugin:

Devido aos recursos necessários para a trilha de auditoria, em alguns casos, apenas uma trilha de auditoria parcial será fornecida. A trilha de auditoria completa está disponível para um único host verificado. Se entre 2 e 512 hosts forem verificados, uma trilha de auditoria completa estará disponível somente se o servidor Nessus tiver mais de uma CPU e 2G de memória RAM. A varredura superior a 512 hosts sempre resultará em uma trilha de auditoria parcial.

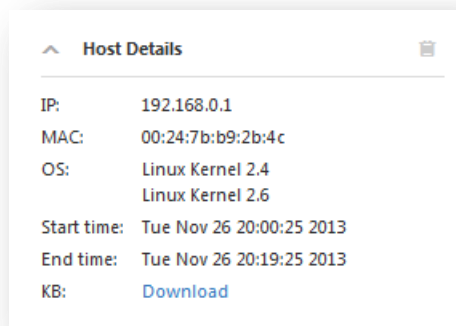
A trilha de auditoria está disponível somente para varreduras originadas no host. Ela não funciona em varreduras importadas.

Capturas de tela de relatórios

O Nessus 5.2 também tem a capacidade de capturar telas durante uma varredura de vulnerabilidade e incluí-las em um relatório. Por exemplo, se o Nessus detectar um VNC executando sem uma senha para restringir o acesso, uma captura poderá ser realizada para mostrar a sessão e ser incluída no relatório. No exemplo abaixo, um VNC foi detectado onde o usuário estava navegando em um site Tenable:

Este recurso deve estar ativado na seção “**Preferences**” (Preferências) de uma política de varredura, em “**Remote Web server screenshot**” (Captura de tela de servidor Web remoto). Consulte a seção Como verificar detalhes de preferências neste documento para obter mais informações.

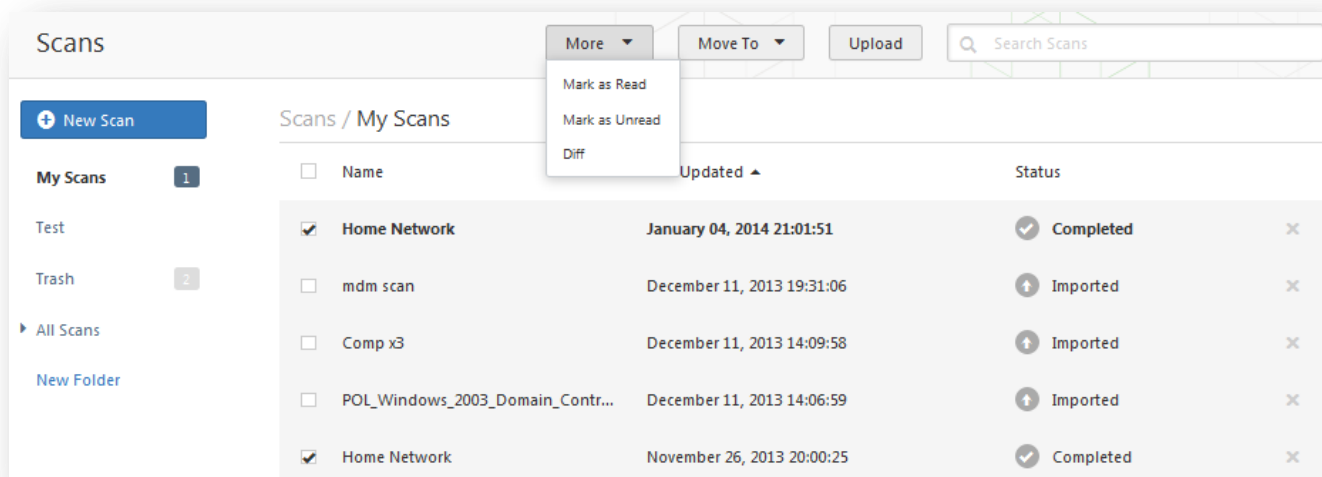
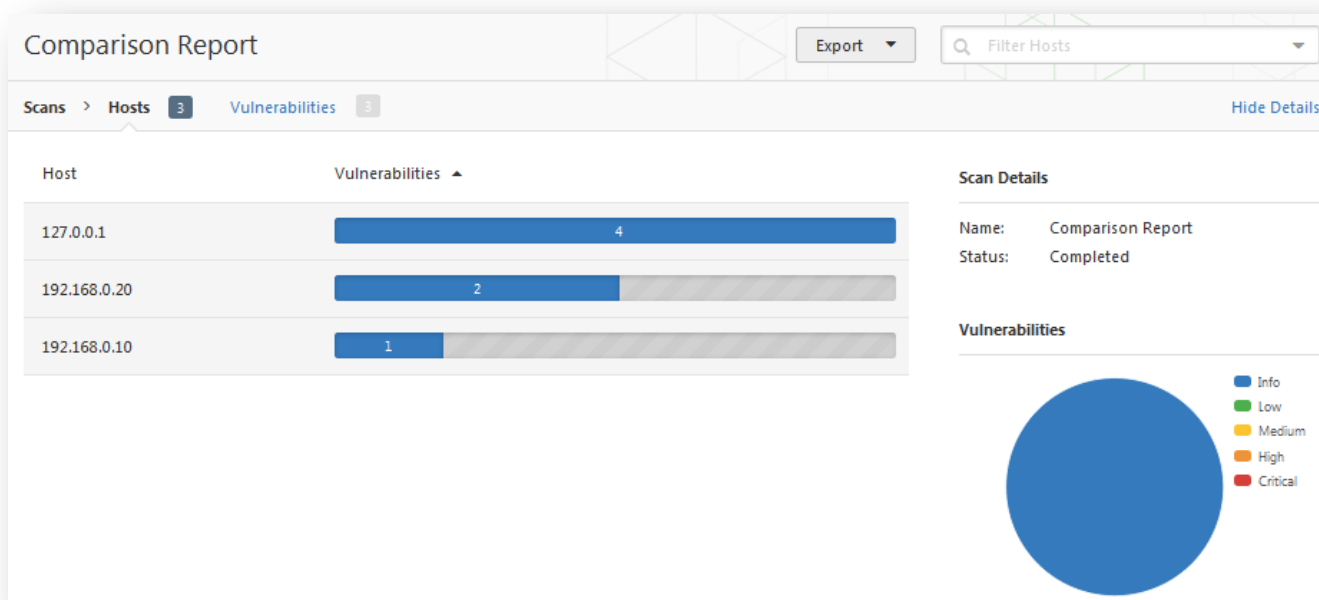
Base de conhecimento de varreduras

Uma Base de conhecimento (KB) é salva a cada varredura realizada. Este é um arquivo de texto ASCII que contém um registro de informações correspondentes para a varredura realizada e os resultados encontrados. Uma base de conhecimento é normalmente útil nos casos em que é necessário suporte da Tenable, uma vez que permite que a equipe de suporte entenda exatamente o comportamento do Nessus e as informações encontradas.

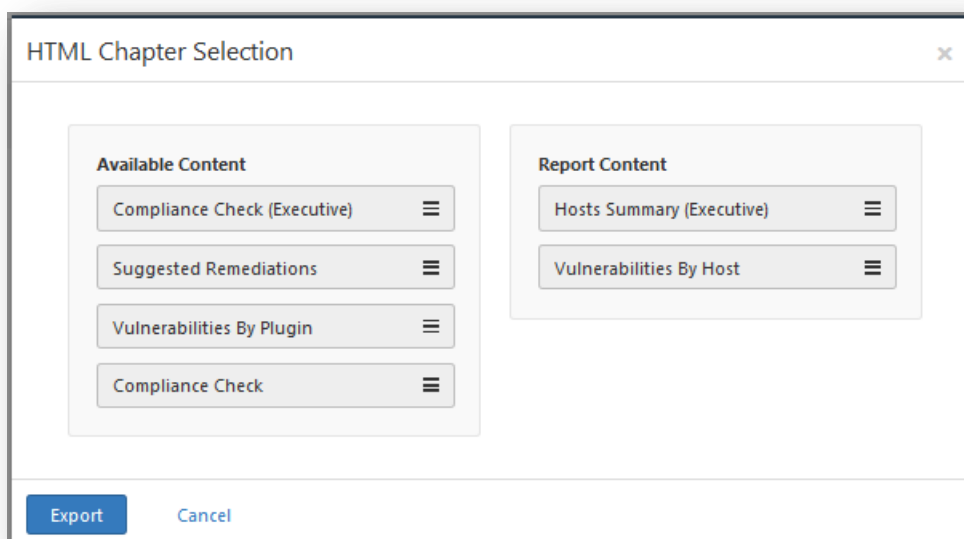
Para fazer download de uma KB, selecione um relatório e, depois, um host específico. À direita do nome do host ou do IP, há um link chamado “**Host Details**” (Detalhes do host). Clique nele. Um dos detalhes do host é “**KB**” com um link de “**Download**” (Baixar):

Somente varreduras realizadas no host terão uma KB associada. Varreduras importadas não possuem KBs com elas.

Compare (Diff Results) (Comparar - Resultados diferentes)

Com o Nessus, é possível comparar dois relatórios de varredura para exibir as diferenças. A capacidade de exibir as diferenças de varredura ajuda a indicar as mudanças de um determinado sistema ou rede ao longo do tempo. Isto permite analisar a conformidade ao mostrar como as vulnerabilidades são corrigidas, se os sistemas recebem correções à medida que novas vulnerabilidades são encontradas ou se duas varreduras estão direcionadas aos mesmos hosts.

Para comparar relatórios, selecione duas varreduras da lista "**Scans**" (Varreduras), clique em "**More**" (Mais) e selecione "**Diff**" (Diferente) no menu suspenso:

O Nessus irá comparar o primeiro relatório selecionado com o segundo e produzir uma lista de resultados diferentes do primeiro. O recurso de comparação mostra o que há de novo na linha de base (ou seja, o primeiro relatório selecionado), mas não produz um diferencial de dois relatórios. A comparação destaca as vulnerabilidades descobertas e corrigidas entre as duas varreduras. No exemplo acima, "DMZ Web Server" (Servidor Web DMZ) é uma varredura sem autenticação de um servidor Web único em um DMZ, realizada diversas vezes. Os resultados exibem as diferenças, destacando as vulnerabilidades que não foram encontradas na varredura de 7 de outubro:

Upload (Fazer upload) e Export (Exportar)

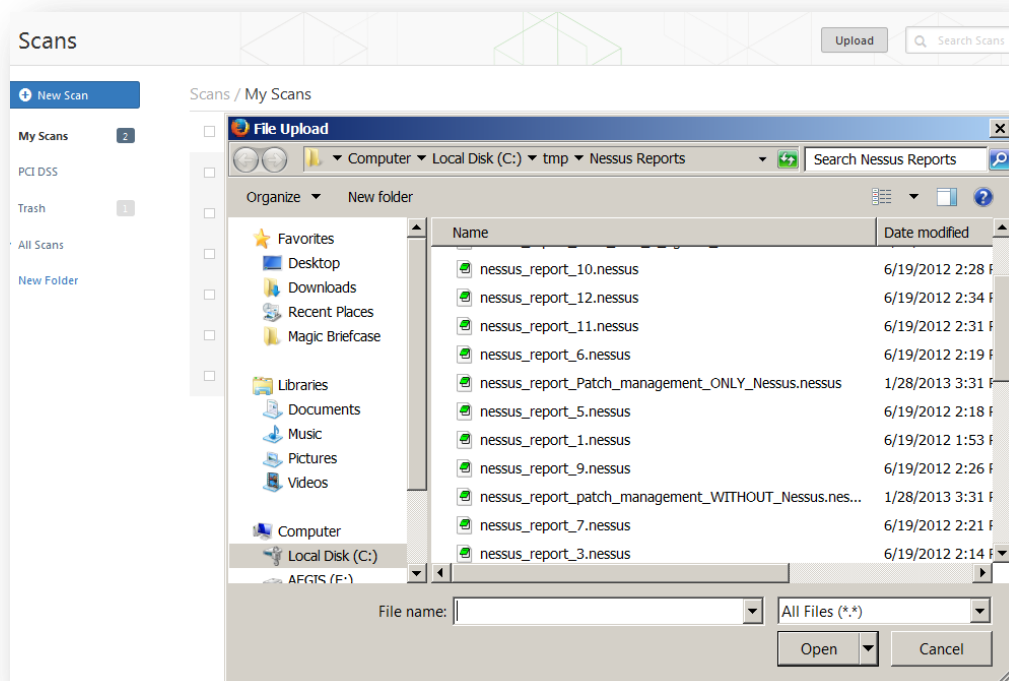
Os resultados das varreduras podem ser exportados de um scanner Nessus e importados em outro scanner Nessus. Os recursos “**Upload**” (Fazer upload) e “**Export**” (Exportar) facilitam o gerenciamento das varreduras, a comparação de relatórios, o backup de relatórios e a comunicação entre grupos ou organizações em uma empresa.

Para exportar uma varredura, selecione o relatório na tela “**Scans**” (Varreduras), clique no menu suspenso “**Export**” (Exportar) na parte superior e escolha o formato desejado. Esta ação exibirá uma janela que permitirá a especificação das informações (divididas em "capítulos") a serem incluídas. À esquerda, há o conteúdo disponível e, à direita há o conteúdo que será exportado. É possível arrastar o conteúdo de um lado para outro para criar um relatório personalizado:

As varreduras de conformidade realizadas com o Nessus 5 podem ser exportadas para os formatos PDF ou HTML com os capítulos de conformidade. As varreduras importadas de versões anteriores do Nessus não serão exportadas desta maneira.

Os relatórios podem ser baixados em vários formatos. Observe que alguns formatos não permitirão a seleção de capítulos ou incluirão todas as informações.

Opção	Descrição
`.nessus`	Um formato do tipo XML, padrão do Nessus 4.2 e versões posteriores. Este formato usa um conjunto extenso de tags XML, que tornam a extração e a análise de informações mais granular. Este relatório não permite selecionar o capítulo.
`.nessus` **(v1)**	Um formato do tipo XML usado do Nessus 3.2 ao 4.0.2, compatível com o Nessus 4.x e Security Center 3. Este relatório não permite selecionar o capítulo.
HTML	Relatório gerado utilizando HTML padrão que permite selecionar o capítulo. Este relatório será aberto em uma nova guia do navegador.
PDF	Relatório gerado em formato PDF que permite selecionar o capítulo. Dependendo do tamanho do relatório, a geração de PDF pode levar vários minutos. O Oracle Java (conhecido como Java da Sun Microsystems) é necessário para a funcionalidade de relatórios no formato PDF.
CSV	Exportação em valores separados por vírgulas, que pode ser usada para importação em muitos programas externos, como bancos de dados, planilhas e outros. Este relatório não permite selecionar o capítulo.

Depois de selecionar um formato, a caixa de diálogo “**Save File**” (Salvar Arquivo) do navegador será exibida, permitindo que o usuário salve os resultados da varredura no local de sua escolha.

Para importar um relatório, clique no botão “**Upload**” (Fazer upload) na barra superior da tela “**Scans**” (Varreduras) para abrir uma janela de navegação de arquivos:

Selecione o arquivo de varredura **`.nessus`** que deseja importar e clique em “**Open**” (Abrir). O Nessus analisará as informações e as disponibilizará na interface “**Scans**” (Varreduras).

Formato de arquivo .nessus

O Nessus usa um formato de arquivo específico (**`.nessus`**) para importar e exportar varreduras. Este formato tem as seguintes vantagens:

- É um arquivo do tipo XML compatível com versões anteriores e futuras e facilita a implementação.
- Autossuficiente: um único arquivo **`.nessus`** contém a lista de alvos e as políticas definidas pelo usuário, além dos próprios resultados da varredura.
- Seguro: as senhas não são salvas no arquivo. Em vez disso, usa-se uma referência a uma senha armazenada em um local seguro no host local.

O processo de criação de um arquivo **`.nessus`** que contém os alvos, as políticas e os resultados das varreduras é, primeiramente, gerar a política e salvá-la. Em seguida, gerar a lista de endereços de destino e, por último, executar uma varredura. Quando a varredura for concluída, todas as informações poderão ser salvas em um arquivo **`.nessus`** com a opção “**Export**” (Exportar) do resultado de “**Scans**” (Varreduras). Consulte o documento “Nessus v2 File Format” (Formato de Arquivo Nessus v2) para obter mais detalhes sobre os arquivos **`.nessus`**.

Delete (Excluir)

Quando os resultados de varredura estiverem concluídos, clique no “X” à direita da varredura na guia “**Scans**” (Varreduras):

Essa ação não pode ser desfeita. Use o recurso “**Export**” (Exportar) para exportar os resultados de varredura antes da exclusão.

Mobile (Móvel)

O Nessus 5 tem a capacidade de varrer Active Directory Service Interfaces (Interfaces de serviço de diretório ativo) e Apple Profile Manager (Gerenciador de perfis Apple), permitindo a varredura de inventário e vulnerabilidade de dispositivos com base em iOS da Apple ou Android. O Nessus pode ser configurado para autenticar nesses servidores, consultar informações de dispositivos móveis e reportar questões.

Para procurar dispositivos móveis, o Nessus deve ser configurado com informações de autenticação para o(s) servidor(es) de gerenciamento.

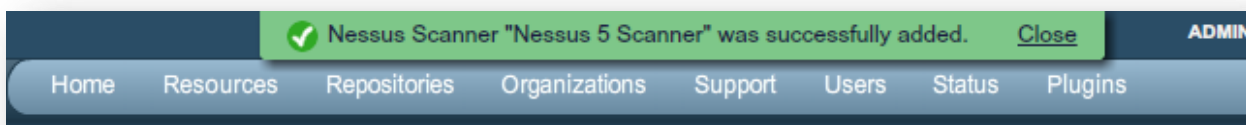
A funcionalidade de varredura Mobile (Móvel) é especificada no menu “**Configuration**” (Configuração). A guia “**Mobile Settings**” (Configurações de dispositivo móvel) contém um espaço para configurar as informações do Apple Profile Manager e ADSI. Como o Nessus autentica diretamente com os servidores de gerenciamento, uma política de varredura móvel será criada automaticamente com a família de plugins Mobile (Móvel) ativada e uma varredura Mobile (Móvel) será criada em “**Templates**” (Modelos). Usando a varredura modelo, os dispositivos móveis podem ser examinados com a frequência necessária.

SecurityCenter

Configuração do SecurityCenter para funcionar com o Nessus

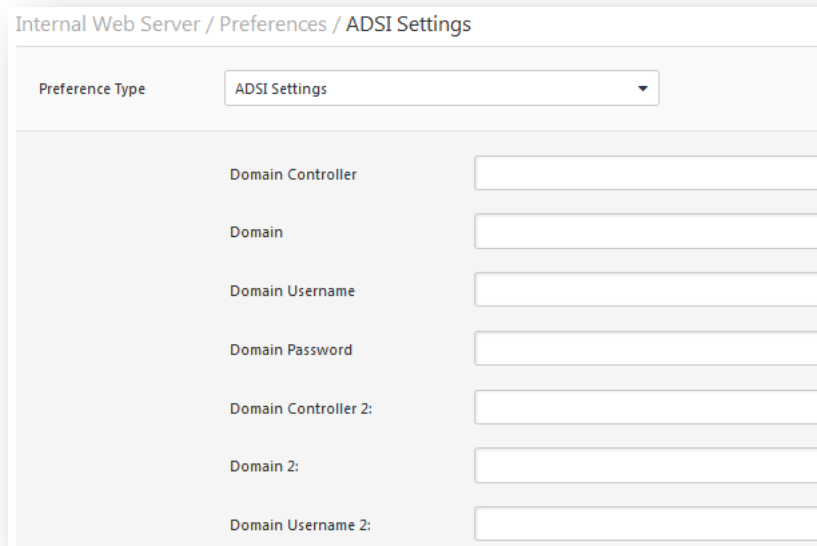
A interface de administração do SecurityCenter é usada para configurar o acesso e controlar qualquer scanner Nessus, ou seja, versão 4.2.x ou superior. Clique na guia “**Resources**” (Recursos) e clique em “**Nessus Scanners**” (Scanners Nessus). Clique em “**Add**” (Adicionar) para abrir a caixa de diálogo **“Add Scanner”** (Adicionar scanner). O endereço IP ou nome do host do scanner Nessus, a porta do Nessus (padrão: 8834), as informações sobre o tipo de autenticação (criado durante a configuração do Nessus), a ID de login com status de administrador e a senha são obrigatórios. Os campos de senha não estarão disponíveis se a autenticação “**SSL Certificate**” (Certificado SSL) for selecionada. A capacidade de verificar o nome do host é fornecida para verificação do CommonName (CN) do certificado SSL apresentado pelo servidor Nessus. O estado do scanner Nessus pode ser definido como ativado ou desativado, conforme necessário. O uso de um proxy pode ser selecionado e a seleção das Scan Zones (Áreas de varredura) às quais o scanner Nessus é atribuído pode ser realizada.

Um exemplo de imagem da página “**Add Scanner**” (Adicionar scanner) do SecurityCenter 4.7 é mostrado abaixo:

Depois de adicionar o scanner com êxito, o banner a seguir é exibido:

Para obter mais informações sobre como integrar o Nessus ao SecurityCenter, consulte o “SecurityCenter Administration Guide” (Guia de Administração do SecurityCenter), disponível no Tenable Support Portal (Portal de suporte da Tenable).

Firewalls instalados no host

Se o servidor Nessus estiver configurado com um firewall local como Zone Alarm, BlackICE, firewall do Windows XP ou qualquer outro software de firewall, será necessário que as conexões sejam permitidas a partir do endereço IP do SecurityCenter.

Normalmente, a porta 8834 é usada para a comunicação com o SecurityCenter. Nos sistemas Microsoft XP Service Pack 2 e posteriores, clicar no ícone “**Central de Segurança**” no “**Painel de Controle**” permite gerenciar as configurações da opção “Firewall do Windows”. Para abrir a porta 8834, selecione a guia “**Exceções**” e adicione a porta “8834” à lista.

Verificação de preferências detalhadas

A guia "**Preferences**" (Preferências) em "**Policies**" (Políticas) contém 40 menus de controle individualizados para configuração de varreduras. Recomenda-se reservar algum tempo para explorar e configurar cada menu para obter mais flexibilidade e resultados de verificação mais precisos com relação à política padrão. A seção a seguir oferece mais detalhes sobre cada opção "**Preferences**" (Preferências). Observe que essa é uma lista dinâmica de opções de configuração e depende da versão do Nessus, das políticas de auditoria e de outras funções às quais o scanner Nessus conectado tem acesso. Uma versão comercial do scanner pode ter opções de configuração mais avançadas do que o Nessus Home. Esta lista também pode mudar à medida que os plugins são adicionados ou modificados.

ADSI Settings (Configurações de ADSI)

O menu "**ADSI Settings**" (Configurações de ADSI) permite que o Nessus solicite a um servidor ActiveSync determinar se dispositivos Android ou iOS estão conectados. Usando as credenciais e as informações de servidor, o Nessus autentica no controlador de domínio (não no servidor Exchange) para consultá-lo diretamente sobre informações de dispositivos. Esse recurso não exige que quaisquer portas sejam especificadas na política de varredura. Essas configurações são obrigatórias para varreduras de dispositivos móveis. O Nessus coletará informações de qualquer telefone que tiver sido atualizado via ADSI nos últimos 365 dias.

Obs.: para "**ADSI Settings**" (Configurações de ADSI), "**Apple Profile Manager API Settings**" (Configurações de API do Apple Profile Manager) e "**Good MDM Settings**" (Configurações de Good MDM), os dispositivos de host não precisam ser varridos diretamente para se obter informações sobre eles. O scanner Nessus deve ser capaz de alcançar o servidor MDM para consultá-lo quanto a informações. Quando alguma dessas opções for configurada, a política de varredura não solicitará um host de destino para varredura; é possível usar "localhost" como destino e a política ainda alcançará o servidor MDM para obter informações.

Apple Profile Manager API Settings (Configurações de API Apple Profile Manager)

O menu "**Apple Profile Manager API Settings**" (Configurações de API do Apple Profile Manager) permite que o Nessus solicite um servidor do Apple Profile Manager para enumerar dispositivos Apple com base em iOS (por exemplo: iPhone, iPad) na rede. Usando as credenciais e as informações de servidor, o Nessus autentica no Profile Manager para consultá-lo diretamente sobre informações de dispositivos. Ou então, é possível especificar comunicações por SSL, assim como direcionar o servidor para forçar uma atualização de informações de dispositivos (ou seja, cada dispositivo atualizará suas informações no servidor do Profile Manager).

Esse recurso não exige que quaisquer portas sejam especificadas na política de varredura. Essas configurações são obrigatórias para varreduras de dispositivos móveis.

Check Point GAiA Compliance Checks (Verificações de conformidade Check Point GAiA)

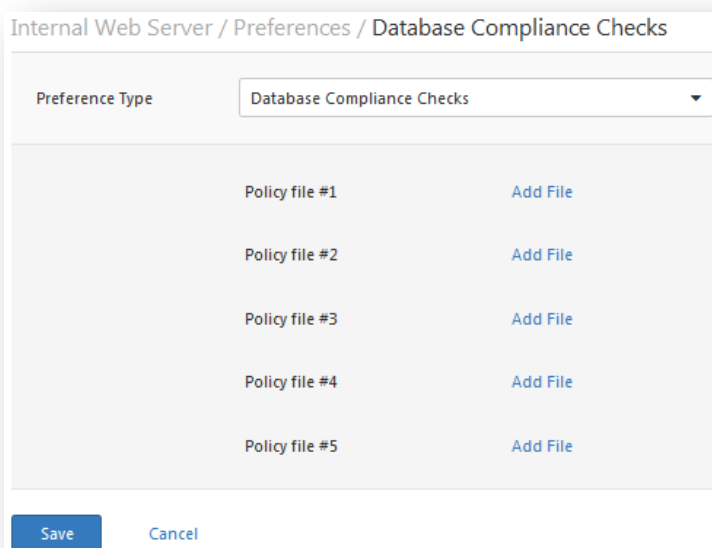
O menu "**Check Point GAiA Compliance Checks**" (Verificações de conformidade Check Point GAiA) permite que clientes comerciais enviem arquivos de políticas que serão usados para determinar se um dispositivo com base em Check Point GAiA atende aos padrões de conformidade especificados. Até cinco políticas podem ser selecionadas ao mesmo tempo.

Cisco IOS Compliance Checks (Verificações de conformidade Cisco IOS)

O menu **"Cisco IOS Compliance Checks**" (Verificações de conformidade Cisco IOS) permite que clientes comerciais enviem arquivos de políticas que serão usados para determinar se um dispositivo Cisco IOS verificado atende aos

padrões de conformidade especificados. Até cinco políticas podem ser selecionadas ao mesmo tempo. As políticas podem ser aplicadas com base nas configurações Saved (Salvo) (**`show config`**), Running (Em execução) (**`show running`**) ou Startup (Inicialização) (**`show startup`**).

Citrix XenServer Compliance Checks (Verificações de conformidade Citrix XenServer)

O menu "**Citrix XenServer Compliance Checks**" (Verificações de conformidade Citrix XenServer) permite que clientes comerciais enviem arquivos de políticas que serão usados para determinar se um sistema XenServer verificado atende aos padrões de conformidade especificados. Até cinco políticas podem ser selecionadas ao mesmo tempo.

Database Compliance Checks (Verificações de conformidade de banco de dados)

O menu "**Database Compliance Checks**" (Verificações de conformidade de banco de dados) permite que clientes comerciais enviem arquivos de políticas que serão usados para determinar se um banco de dados testado atende aos padrões de conformidade especificados. Até cinco políticas podem ser selecionadas ao mesmo tempo.

Database settings (Configurações de banco de dados)

As opções "**Database settings**" (Configurações de banco de dados) são usadas para especificar o tipo de banco de dados a ser verificado e as configurações e credenciais correspondentes:

Opção	Descrição
Login	O nome de usuário do banco de dados.
Password (Senha)	A senha para o nome de usuário fornecido.
DB Type (Tipo de BD)	Oracle, SQL Server, MySQL, DB2, Informix/DRDA e PostgreSQL são permitidos.
Database SID (SID do banco de dados)	ID do banco de dados para auditoria.
Database port to use (Porta do banco de dados para usar)	Porta de escuta do banco de dados.
Oracle auth type (Tipo aut Oracle)	NORMAL, SYSOPER e SYSDBA são permitidos.
SQL Server auth type (Tipo aut SQL Server)	Windows ou SQL são permitidos.

Do not scan fragile devices (Não verificar dispositivos frágeis)

O menu "**Do not scan fragile devices**" (Não verificar dispositivos frágeis) oferece duas opções que instruem o scanner Nessus a não verificar um histórico de "fragilidade" ou propensão a falhas ao receber uma entrada inesperada. Os usuários podem selecionar "**Scan Network Printers**" (Verificar impressoras em rede) ou "**Scan Novell Netware hosts**" (Verificar hosts Novell Netware) para instruir o Nessus a verificar esses dispositivos específicos. O Nessus só poderá verificar esses dispositivos se essas opções estiverem marcadas. Recomenda-se que a verificação desses dispositivos seja realizada de maneira a permitir às equipes de TI monitorar problemas nos sistemas.

FireEye Compliance Checks (Verificações de conformidade FireEye)

O menu “**FireEye Compliance Checks**” (Verificações de conformidade FireEye) permite que clientes comerciais enviem arquivos de políticas que serão usados para determinar se um dispositivo FireEye testado atende aos padrões de conformidade especificados. Até cinco políticas podem ser selecionadas ao mesmo tempo.

Global variable settings (Configurações globais de variáveis)

O menu “**Global variable settings**” (Configurações globais de variáveis) contém uma grande variedade de opções de configuração para o servidor Nessus.

A tabela a seguir fornece informações detalhadas sobre cada opção disponível:

Opção	Descrição
Probe services on every port (Investigar serviços em cada porta)	Relaciona cada porta aberta ao serviço que está sendo executado na porta. Observe que, em alguns casos raros, isto pode prejudicar alguns serviços e causar efeitos colaterais inesperados.
Do not log in with user accounts not specified in the policy (Não fazer login em contas de usuário não especificadas na política)	Usado para evitar o bloqueio de contas se a política de senhas estiver definida para bloquear as contas depois de algumas tentativas inválidas.
Enable CGI scanning (Ativar varredura de CGI)	Ativa a varredura de CGI. Desative esta opção para acelerar a auditoria de uma rede local.

Network type (Tipo de rede)	Permite especificar se você está usando IPs públicos roteáveis, IPs roteáveis privados não pertencentes à Internet ou uma combinação de ambos. Selecione “Mixed” (Combinado) se os endereços RFC 1918 forem usados com diversos roteadores de rede.
Enable experimental scripts (Ativar scripts experimentais)	Faz com que os plugins "em teste" sejam usados na varredura. Não ative esta opção durante a varredura de uma rede de produção.
Thorough tests (slow) (Testes completos (lento))	Permite que os plugins realizem testes "completos". Por exemplo: ao examinar compartilhamentos de arquivos SMB, um plugin pode analisar com três níveis de profundidade em vez de 1. Isto pode aumentar o tráfego da rede e as análises, em alguns casos. Observe que, por ser mais completa, a varredura deve ser mais invasiva e é mais provável que afete a rede, mas os resultados de auditoria podem ser melhores.
Report verbosity (Detalhamento do relatório)	Um valor mais alto gerará mais informações sobre a atividade do plugin no relatório.
Report paranoia (Sensibilidade do relatório)	Em alguns casos, o Nessus não pode determinar remotamente se uma falha está presente ou não. Se a sensibilidade do relatório for definida como “**Paranoid**” (Sensível), uma falha sempre será relatada, mesmo se houver dúvidas sobre o host remoto afetado. Por outro lado, a configuração de sensibilidade “**Avoid false alarm**” (Evitar alarmes falsos) fará com que o Nessus não comunique nenhuma falha sempre que houver uma sombra de incerteza sobre o host remoto. A opção padrão (“**Normal**”) é a configuração padrão entre as configurações acima.
HTTP User-Agent (Usuário-Agente HTTP)	Especifica o tipo de navegador que o Nessus representará durante a varredura.
SSL certificate to use (Certificado SSL para usar)	Permite que o Nessus use certificado SSL no lado cliente para se comunicar com um host remoto.
SSL CA to trust (CA SSL para confiabilidade)	Especifica a Autoridade Certificadora (CA) para confiabilidade do Nessus.
SSL key to use (Chave SSL para usar)	Especifica uma chave SSL local que será usada para se comunicar com o host remoto.
SSL password for SSL key (Senha SSL para chave SSL)	A senha usada para gerenciar a chave SSL especificada.

Good MDM Settings (Configurações de Good MDM)

O menu “**Good MDM Settings**” (Configurações de Good MDM) permite que o Nessus solicite a um servidor de gerenciamento de dispositivos móveis Good determinar se dispositivos Android ou iOS estão conectados. Usando as credenciais e as informações de servidor, o Nessus autentica no servidor GMC para consultá-lo diretamente sobre informações de dispositivos. Esse recurso não exige que quaisquer portas sejam especificadas na política de varredura. Essas configurações são obrigatórias para varreduras de dispositivos móveis.

Obs.: para “**ADSI Settings**” (Configurações de ADSI), “**Apple Profile Manager API Settings**” (Configurações de API do Apple Profile Manager) e “**Good MDM Settings**” (Configurações de Good MDM), os dispositivos de host não precisam ser varridos diretamente para se obter informações sobre eles. O scanner Nessus deve ser capaz de alcançar o servidor MDM (Mobile Device Management) para consultá-lo quanto a informações. Quando alguma dessas opções for configurada, a política de varredura não solicitará um host de destino para varredura: é possível usar "localhost" como destino e a política ainda alcançará o servidor MDM para obter informações.

HP ProCurve Compliance Checks (Verificações de conformidade HP ProCurve)

O menu "**HP ProCurve Compliance Checks**" (Verificações de conformidade HP ProCurve) permite que clientes comerciais enviem arquivos de políticas que serão usados para determinar se um dispositivo HP ProCurve testado atende aos padrões de conformidade especificados. Até cinco políticas podem ser selecionadas ao mesmo tempo.

HTTP cookies import (Importação de cookies HTTP)

Para facilitar os testes de aplicativos da Web, o Nessus pode importar cookies HTTP de outro software (por exemplo: navegador, proxy da Web etc.) com as configurações "**HTTP cookies import**" (Importação de cookies HTTP). Um

arquivo de cookie pode ser enviado para que o Nessus utilize cookies para acessar um aplicativo da Web. O arquivo do cookie deve estar no formato Netscape.

HTTP login page (Página de login HTTP)

As configurações "**HTTP login page**" (Página de login HTTP) permitem controlar o local em que os testes autenticados de um aplicativo personalizado baseado na Web têm início.

Opção	Descrição
Login page (Página de login)	O caminho absoluto para a página de login do aplicativo, por exemplo: "/login.html".
Login form (Formulário de login)	O parâmetro "action" do método do formulário. Por exemplo, o formulário de login de `<form method="POST" name="auth_form" action="/login.php">` seria "`/login.php`".
Login form fields (Campos do formulário de login)	Especifique os parâmetros de autenticação (por exemplo: `login=%USER%&password=%PASS%`). Se as palavras-chaves %USER% e %PASS% forem usadas, serão substituídas por valores fornecidos no menu suspenso "Login configurations" (Configurações de login). Este campo pode ser usado para fornecer mais de dois parâmetros, se necessário (por exemplo: um nome de "grupo" ou alguma outra informação é necessária para o processo de autenticação).
Login form method (Método do formulário de login)	Especifica se a ação de login é realizada por meio de uma solicitação GET ou POST.
Automated login page search (Pesquisa automática de página de login)	Instrui o Nessus a pesquisar uma página de login.
Re-authenticate delay (seconds) (Intervalo de reautenticação (s))	O intervalo entre as tentativas de autenticação. Previne o acionamento de mecanismos de bloqueio por força bruta.
Check authentication on page (Verificar autenticação na página)	O caminho absoluto de uma página da Web protegida que requer autenticação para ajudar o Nessus a definir o status de autenticação, por exemplo: "/admin.html".
Follow 30x redirections (# of levels) (Seguir redirecionamentos 30x (nº	Se um código de redirecionamento 30x for recebido de um servidor da Web, isso instruirá o Nessus a seguir o link fornecido ou não.

de níveis))	
Authenticated regex (Regex autenticado)	Um padrão regex para pesquisa na página de login. O recebimento de um código de resposta 200 nem sempre é suficiente para determinar o estado da sessão. O Nessus pode tentar localizar uma determinada string, como “Authentication successful!” (Autenticação bem-sucedida).
Invert test (disconnected if regex matches) (Inverter teste (desconectar se houver correspondências regex))	Um padrão regex para pesquisa na página de login. Se for encontrado, indica ao Nessus que a autenticação não teve êxito (por exemplo: “Authentication failed!”).
Match regex on HTTP headers (Corresponder regex em cabeçalhos HTTP)	O Nessus pode pesquisar um determinado padrão regex nos cabeçalhos de resposta HTTP para definir melhor o estado de autenticação, em vez de pesquisar no corpo de uma resposta.
Case insensitive regex (Regex não diferencia maiúsculas de minúsculas)	Normalmente, as pesquisas por regex diferenciam maiúsculas de minúsculas. O comando instrui o Nessus a ignorar a diferenciação.
Abort Web application tests if login fails (Interromper testes de aplicativos da Web se login falhar)	Se as credenciais fornecidas não funcionarem, o Nessus interromperá os testes personalizados de aplicativos da Web, mas não as famílias de plugins de CGI.

Internal Web Server / Preferences / HTTP login page
Preference Type
HTTP login page
Login page
/
Login form
Login form fields
user=%USER%&pass=%PASS%
Login form method
POST
Automated login page search
Re-authenticate delay (seconds)
Check authentication on page
Follow 30x redirections (# of levels)
2
Authenticated regex
Invert test (disconnected if regex matches)
Match regex on HTTP headers
Case insensitive regex
Abort web application tests if login fails
Save
Cancel

IBM iSeries Compliance Checks (Verificações de conformidade IBM iSeries)

O menu "**IBM iSeries Compliance Checks**" (Verificações de conformidade IBM iSeries) permite que clientes comerciais enviem arquivos de políticas que serão usados para determinar se um sistema IBM iSeries atende aos padrões de conformidade especificados. Até cinco políticas podem ser selecionadas ao mesmo tempo.

IBM iSeries Credentials (Credenciais para IBM iSeries)

As preferências de "**IBM iSeries Credentials**" (Credenciais para IBM iSeries) proporcionam um local para que o Nessus forneça credenciais para autenticação do sistema IBM iSeries. Isto é necessário para auditorias de conformidade, por exemplo.

ICCP/COTP TSAP Addressing (Endereçamento ICCP/COTP TSAP)

O menu "**ICCP/COTP TSAP Addressing**" (Endereçamento ICCP/COTP TSAP) está relacionado especificamente às verificações Scada. O menu determina um valor de Pontos de Acesso de Serviço de Transporte (TSAP) do protocolo de Transporte Orientado a Conexões (COTP) em um servidor ICCP. Os valores de início e parada são definidos inicialmente como "8".

Juniper Junos Compliance Checks (Verificações de conformidade Juniper Junos)

O menu "**Juniper Junos Compliance Checks**" (Verificações de conformidade Juniper Junos) permite que clientes comerciais enviem arquivos de políticas que serão usados para determinar se um dispositivo Juniper Junos testado atende aos padrões de conformidade especificados. Até cinco políticas podem ser selecionadas ao mesmo tempo.

LDAP 'Domain Admins' Group Membership Enumeration (Escalonamento de privilégios de membro de grupo de "admin. de domínio" LDAP)

O menu "**LDAP 'Domain Admins' Group Membership Enumeration**" (Escalonamento de privilégios de membro de grupo de "admin. de domínio" LDAP) permite inserir um conjunto de credenciais LDAP que podem ser usados para enumerar uma lista de membros do grupo "Domain Admins" no diretório LDAP remoto.

Login configurations (Configurações de Login)

O menu “**Login configurations**” (Configurações de Login) permite que o scanner Nessus use credenciais ao verificar HTTP, NNTP, FTP, POP2, POP3 ou IMAP. Ao fornecer credenciais, o Nessus pode realizar verificações mais abrangentes para determinar as vulnerabilidades. As credenciais de HTTP fornecidas aqui serão usadas apenas para autenticação básica e resumida. Para configurar as credenciais de um aplicativo da Web personalizado, use o menu suspenso “HTTP login page” (Página de login HTTP).

Internal Web Server / Preferences / Login configurations

Preference Type: Login configurations

HTTP account

HTTP password (sent in clear)

NNTP account

NNTP password (sent in clear)

FTP account: anonymous

FTP password (sent in clear): ••••••••••••••••

FTP writeable directory: /incoming

POP2 account

POP2 password (sent in clear)

POP3 account

POP3 password (sent in clear)

IMAP account

IMAP password (sent in clear)

Save Cancel

Malicious Process Detection (Detecção de processo malicioso)

O menu “**Malicious Process Detection**” (Detecção de processo malicioso) permite a especificação de uma lista de hashes MD5 que o Nessus usará para verificar um sistema em busca de malwares conhecidos. Essa lista é usada pelo plugin “Malicious Process Detection: User Defined Malware Running” (ID do plugin 65548), que funciona como o “Malicious Process Detection” (Plugin ID 59275) do Tenable. Hashes adicionais podem ser enviados através de um arquivo de texto que contém um hash MD5 por linha. É possível (opcional) adicionar uma descrição para cada hash no arquivo carregado. Isso é realizado adicionando uma vírgula após o hash, seguida pela descrição. Se alguma correspondência for encontrada durante a verificação de um destino, e uma descrição for fornecida ao hash, a descrição aparecerá nos resultados da varredura. Comentários com base em hash (por exemplo: #) podem ser usados opcional e adicionalmente com os delimitados por vírgulas.

Modbus/TCP Coil Access (Acesso Modbus/TCP Coil)

As opções de “**Modbus/TCP Coil Access**” (Acesso Modbus/TCP Coil) estão disponíveis para usuários comerciais. Este item do menu suspenso é gerado dinamicamente pelos plugins SCADA disponíveis com a versão comercial do Nessus. O Modbus usa o código de função 1 para ler “bobinas” em um escravo Modbus. As bobinas representam configurações de saída binárias e normalmente são correlacionadas com atuadores. A capacidade de ler bobinas pode ajudar um atacante a criar um perfil do sistema, identificar intervalos de registros e alterá-los por meio de uma mensagem “write coil” (gravar bobina). Os valores padrão são “0” para o reg Start e “16” para o reg End.

Nessus SYN scanner and Nessus TCP scanner (Scanner Nessus SYN e scanner Nessus TCP)

As opções “**Nessus SYN scanner**” e “**Nessus TCP scanner**” (Scanner Nessus SYN e scanner Nessus TCP) permitem configurar os scanners SYN e TCP originais para detectar a presença de um firewall.

Valor	Descrição
Automatic (normal) (Automático (normal))	Esta opção pode ajudar a identificar se um firewall está localizado entre o scanner e o destino (**padrão**).
Disabled (softer) (Desabilitado (mais leve))	Desativa o recurso **Firewall detection** (Detecção de firewall).
Do not detect RST rate limitation (soft) (Não detector limitação de taxa de RST (leve))	Desativa a funcionalidade de monitoramento do número de reinícios definidos e determina se há uma limitação configurada por um dispositivo de rede local.

Ignore closed ports (aggressive) (Ignorar portas fechadas (agressivo))	Tenta executar os plugins mesmo que a porta estiver fechada. Recomenda-se que esta opção não seja usada em uma rede de produção.

NetApp Data ONTAP Compliance Checks (Verificações de conformidade NetApp Data ONTAP)

O menu “**NetApp Data ONTAP Compliance Checks**” (Verificações de conformidade NetApp Data ONTAP) permite que clientes comerciais enviem arquivos de políticas que serão usados para determinar se um dispositivo com base em NetApp Data ONTAP verificado atende aos padrões de conformidade especificados. Até cinco políticas podem ser selecionadas ao mesmo tempo.

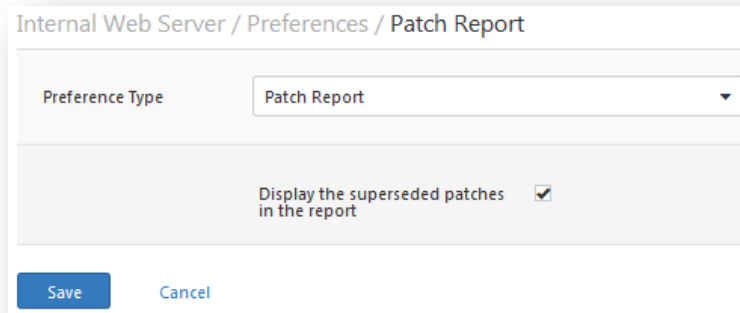
Oracle Settings (Configurações Oracle)

O menu “**Oracle Settings**” (Configurações Oracle) configura o Nessus com o Oracle Database SID (SID de banco de dados Oracle) e inclui uma opção para testar contas padrão conhecidas no software Oracle.

PCI DSS Compliance (Conformidade PCI DSS)

A opção “**PCI DSS Compliance**” (Conformidade PCI DSS) fará com que o Nessus compare os resultados das varreduras com as normas de conformidade PCI DSS vigentes. Este recurso está disponível somente para clientes comerciais.

Patch Management (Gerenciamento de patch)

O Nessus pode explorar credenciais para o servidor Red Hat Satellite, WSUS, SCCM e sistemas de gerenciamento de patches VMware Go (anteriormente Shavlik) para realizar a auditoria de patches nos sistemas nos quais as credenciais não estão disponíveis para o scanner Nessus. As opções dos sistemas de gerenciamento de patches podem ser encontradas em “Preferences” (Preferências) em seus respectivos menus suspensos: “**Patch Management: IBM Tivoli Endpoint Manager Server Settings**” (Gerenciamento de patch: configurações de servidor IBM Tivoli Endpoint Manager), “**Patch Management: Red Hat Satellite Server Settings**” (Gerenciamento de patch: configurações de servidor Satellite Red Hat), “**Patch Management: SCCM Server Settings**” (Gerenciamento de patch: configurações de servidor SCCM), “**Patch Management: VMware Go Server Settings**” (Gerenciamento de patch: configurações de servidor VMware Go) e “**Patch Management: WSUS Server Settings**” (Gerenciamento de patch: configurações de servidor WSUS). Para obter mais informações sobre como utilizar o Nessus para verificar os hosts por meio desses sistemas de gerenciamento de patch, consulte o documento “Patch Management Integration” (Integração de gerenciamento de patches).

Palo Alto Networks PAN-OS Settings (Configurações de Palo Alto Networks PAN-OS)

O menu “**Palo Alto Networks PAN-OS Settings**” (Configurações de Palo Alto Networks PAN-OS) permite que clientes comerciais realizem auditorias de dispositivos Palo Alto PAN-OS. Isso requer credenciais válidas e permite a configuração da porta e, opcionalmente, verificar o certificado SSL por completo antes de continuar.

Patch Report (Relatório de patch)

O menu “**Patch Report**” (Relatório de patch) permite a configuração do Nessus para incluir ou remover informações substituídas de patches no relatório de varredura. Essa opção fica ativada por padrão.

Ping the remote host (Ping para host remoto)

As opções de “**Ping the remote host**” (Ping para host remoto) permitem um controle individualizado sobre a capacidade do Nessus de enviar testes de conexão a hosts durante a varredura de descoberta. Isto pode ser feito com ping ARP, ping TCP, ping ICMP ou ping UDP de aplicativo.

Opção	Descrição
TCP ping destination port(s) (Porta(s) de destino do ping TCP)	Especifica a lista de portas a serem verificadas por meio do teste de ping TCP. Se tiver dúvidas com relação às portas, deixe esta configuração com o valor padrão “interno”.
Number of Retries (ICMP) (Número de novas tentativas (ICMP))	Permite especificar o número de tentativas de ping ao host remoto. O valor padrão é 6.
Do an applicative UDP ping (DNS, RPC…) (Fazer um ping UDP em aplicativo (DNS, RPC…)	Executa um teste de ping UDP em aplicativos específicos que usam UDP, incluindo DNS (porta 53), RPC (porta 111), NTP (porta 123) e RIP (porta 520).
Make the dead hosts appear in the report (Fazer com que os hosts inativos apareçam no relatório)	Se esta opção for selecionada, os hosts que não responderam à solicitação de ping serão incluídos no relatório de segurança como hosts inativos.
Log live hosts in the report (Registrar hosts ativos no relatório)	Selecione esta opção para comunicar especificamente a capacidade de enviar um ping a um host remoto.
Test the local Nessus host (Testar o host Nessus local)	Esta opção permite que o usuário inclua ou exclua o host do Nessus local da varredura. Esta opção é usada quando o host Nessus estiver dentro do intervalo de rede de destino da varredura.
Fast network discovery (Descoberta rápida de rede)	Normalmente, ao enviar um “ping” a um IP remoto com uma resposta, o Nessus realiza varreduras adicionais para verificar se não se trata de um proxy transparente ou um balanceador de carga gerando ruído, mas sem resultado (alguns dispositivos respondem a todas as portas de 1 a 65.535, mas não há nenhum serviço em segundo plano). As verificações podem demorar um pouco, especialmente se o host remoto

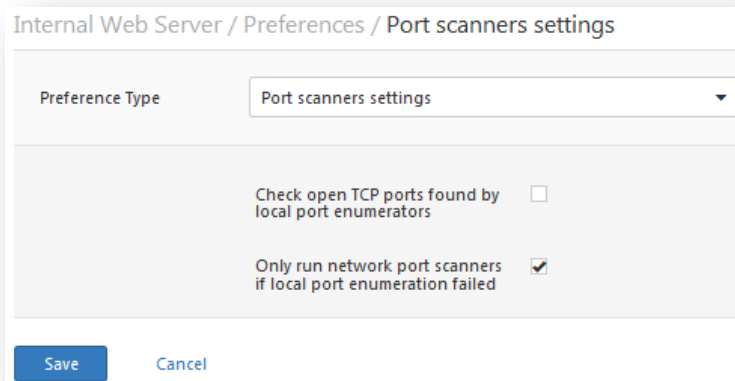
	estiver protegido por um firewall. Se a “fast network discovery” (descoberta rápida de rede) estiver ativada, o Nessus não realizará as varreduras.

Para examinar os sistemas VMware convidados, o “ping” deve ser desativado. Na política de varredura em “Advanced” (Avançado) -> ”Ping the remote host” (Ping para host remoto), desmarque o ping de TCP, ICMP e ARP.

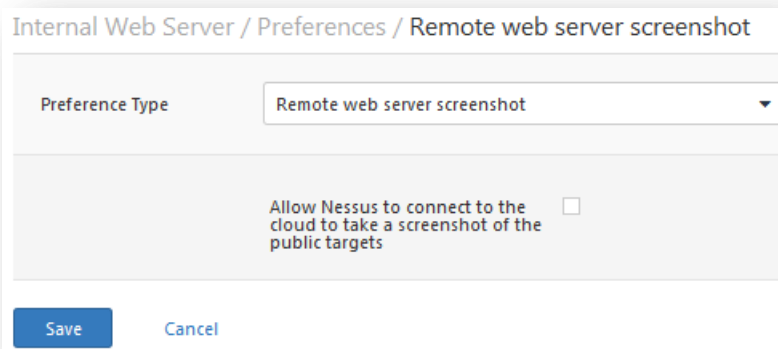
Port scanner settings (Configurações de varredura de portas)

O menu “**Port scanner settings**” (Configurações de varredura de portas) oferece duas opções adicionais para controlar a atividade de varredura de portas:

Opção	Descrição
Check open TCP ports found by local port enumerators (Verificar portas TCP abertas encontradas enumeradores de portas locais)	Se um enumerador de portas locais (por exemplo: WMI ou netstat) encontrar uma porta, o Nessus também verificará se está aberta remotamente. Isto ajuda a determinar se alguma forma de controle de acesso está em uso (por exemplo: TCP wrappers, firewall).
Only run network port scanners if local port enumeration failed (Só	Nesse caso, use primeiro a enumeração de portas locais.

executar varreduras de portas se a enumeração de porta local falhar)	

Remote Web server screenshot (Captura de tela de servidor Web remoto)

O menu “**Remote Web server screenshot**” (Captura de tela de servidor Web remoto) permite que o Nessus capture telas para demonstrar melhor algumas descobertas. Isso inclui alguns serviços (por exemplo: VNC, RDP) assim como opções específicas de configuração (por exemplo, indexação de diretórios de servidor Web). O recurso funciona somente para hosts voltados para a Internet, pois as capturas de tela são geradas em um servidor gerenciado e enviadas ao scanner Nessus.

Observe que as capturas de tela **não** são exportadas com um relatório de varredura Nessus.

SCAP Linux Compliance Checks (Verificações de conformidade SCAP Linux)

O menu “**SCAP Linux Compliance Checks**” (Verificações de conformidade SCAP Linux) permite que clientes comerciais enviem arquivos zip SCAP, que serão usados para determinar se um sistema Linux verificado atende aos padrões de conformidade como especificado na SP 800-126. Para obter mais informações sobre SCAP, visite o site NIST Security Content Automation Protocol (Protocolo de automação de conteúdo de segurança NIST).

SCAP Windows Compliance Checks (Verificações de conformidade SCAP Windows)

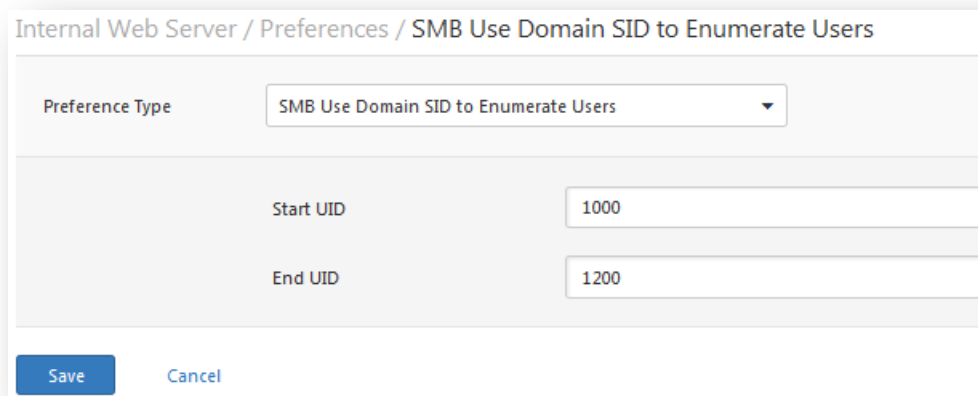
O menu “**SCAP Windows Compliance Checks**” (Verificações de conformidade SCAP Windows) permite que clientes comerciais enviem arquivos zip SCAP, que serão usados para determinar se um sistema Windows verificado atende aos padrões de conformidade como especificado na SP 800-126. Para obter mais informações sobre SCAP, visite o site NIST Security Content Automation Protocol (Protocolo de automação de conteúdo de segurança NIST).

SMB Registry: Start the Registry Service during the scan (Registro SMB: Iniciar o Serviço de Registro durante a varredura)

O menu "**SMB Registry: Start the Registry Service during the scan**" (Registro SMB: Iniciar o Serviço de Registro durante a varredura) permite que o serviço intermedeie algumas das exigências de varredura para computadores em que o registro SMB não esteja sempre em funcionamento.

SMB Registry : Start the Registry Service during the scan (Registro SMB: Iniciar o Serviço de Registro durante a varredura)

O menu "**SMB Registry: Start the Registry Service during the scan**" (Registro SMB: Iniciar o Serviço de Registro durante a varredura) permite que Nessus use credenciais para iniciar temporariamente o serviço SMB Registry (Registro SMB) para que ele realize uma auditoria adicional. Depois de concluir, o Nessus desativará o serviço.

SMB Scope (Alcance do SMB)

No menu "**SMB Scope**" (Alcance do SMB), se a opção "**Request information about the domain**" (Solicitar informações sobre o domínio) estiver selecionada, os usuários do domínio, e não os usuários locais, serão consultados.

SMB Use Domain SID to Enumerate Users (SMB: Usar SID de domínio para enumerar usuários)

O menu "**SMB Use Domain SID to Enumerate Users**" (SMB: Usar SID de domínio para enumerar usuários) especifica o intervalo de SID a ser usado para realizar uma consulta inversa de nomes de usuários no domínio. A configuração padrão é recomendada para a maioria das varreduras.

SMB Use Host SID to Enumerate Local Users (SMB: Usar SID de Host para enumerar usuários locais)

O menu "**SMB Use Host SID to Enumerate Local Users**" (SMB: Usar SID de Host para enumerar usuários locais) especifica o intervalo de SID a ser usado para executar uma consulta inversa de nomes de usuários locais. A configuração padrão é recomendada.

SMTP settings (Configurações SMTP)

O menu "**SMTP settings**" (Configurações SMTP) especifica as opções para os testes de SMTP (Protocolo Simples de Transporte de Correio) executados em todos os dispositivos dentro do domínio verificado que estão executando serviços SMTP. O Nessus tentará retransmitir mensagens por meio do dispositivo ao "**Third party domain**" (Domínio de terceiros) especificado. Se a mensagem enviada ao "**Third party domain**" (Domínio de terceiros) for recusada pelo endereço especificado no campo "**To address**" (Endereço de destino), ocorrerá falha na tentativa de spam. Se a mensagem for aceita, o servidor de SMTP foi usado com sucesso para retransmitir o spam.

Opção	Descrição
Third party domain (Domínio de terceiros)	O Nessus tentará enviar spam por meio de cada dispositivo de SMTP para o endereço listado neste campo. O endereço de domínio de terceiros deve estar fora do intervalo do site que está sendo examinado ou do site que está realizando a varredura. Caso contrário, o teste pode ser interrompido pelo servidor SMTP.
From address (Endereço de envio)	As mensagens de teste enviadas ao(s) servidor(es) SMTP aparecerão como se fossem originadas do endereço especificado neste campo.
To address (Endereço de destino)	O Nessus tentará enviar mensagens endereçadas ao destinatário da mensagem indicado neste campo. O endereço **postmaster** é o valor padrão, pois é um endereço válido na maioria dos servidores de correio.

SNMP settings (Configurações SNMP)

O menu “**SNMP settings**” (Configurações SNMP) permite configurar o Nessus para se conectar e autenticar no serviço SNMP do destino. Durante a varredura, o Nessus fará algumas tentativas de descobrir a string da comunidade e usá-la em testes subsequentes. Até quatro strings de nomes de comunidades separadas podem ser usados por política de varredura. Se o Nessus não localizar a string e/ou a senha da comunidade, não poderá realizar uma auditoria completa do serviço.

Opção	Descrição
Community name (0-3) (Nome da comunidade (0-3))	O nome da comunidade SNMP.
UDP port (Porta UDP)	Instrui o Nessus a verificar uma porta diferente caso o SNMP esteja sendo executado em uma porta que não seja a porta 161.
SNMPv3 user name (Nome de usuário SNMPv3)	O nome de usuário de uma conta que usa SNMPv3.
SNMPv3 authentication password (Senha de autenticação SNMPv3)	A senha do nome de usuário especificado.
SNMPv3 authentication algorithm (Algoritmo de autenticação SNMPv3)	Selecione MD5 ou SHA1, dependendo do algoritmo reconhecido pelo serviço remoto.
SNMPv3 privacy password (Senha de privacidade SNMPv3)	A senha usada para proteger a comunicação SNMP criptografada.
SNMPv3 privacy algorithm (algoritmo de privacidade SNMPv3)	O algoritmo de criptografia a ser usado para o tráfego SNMP.

Service Detection (Detecção de serviço)

O menu "**Service Detection**" (Detecção de serviço) controla o modo como o Nessus testará serviços SSL: portas SSL conhecidas (por exemplo: 443), todas as portas ou nenhuma. O teste de funcionalidade SSL em todas as portas pode afetar o host verificado.

Unix Compliance Checks (Verificações de conformidade Unix)

O menu "**Unix Compliance Checks**" (Verificações de conformidade Unix) permite que clientes comerciais enviem arquivos de auditoria do Unix que serão usado para determinar se um sistema testado atende aos padrões de conformidade especificados. Até cinco políticas podem ser selecionadas ao mesmo tempo.

VMware SOAP API Settings (Configurações de VMware SOAP API)

O menu “**VMware SOAP API Settings**” (Configurações de VMware SOAP API) fornece as credenciais necessárias ao Nessus para autenticação dos sistemas de gerenciamento VMware ESX, ESXi e vSphere Hypervisor por meio do seu próprio SOAP API, uma vez que o acesso SSH foi descontinuado. O API foi projetado para auditoria de hosts do vSphere 4.x / 5.x, ESXi e ESX, mas **não** das máquinas virtuais em funcionamento nos hosts. Este método de autenticação pode ser usado para realizar varredura com credenciais ou auditorias de conformidade.

Opção	Descrição
VMware user name (Nome de usuário VMware)	Nome do usuário para autenticação. As credenciais podem ser contas do Active Directory (AD) para hosts integrados ou contas locais e a conta deve estar no grupo `root` local. As credenciais de domínio são user@domain e as contas locais são usuário e senha.
VMware password (unsafe!) (Senha VMware (insegura!))	Esta senha é enviada de forma insegura e pode ser interceptada por meio de "sniffing" da rede.

Ignore SSL Certificate (Ignorar Certificado SSL)	Se um certificado SSL estiver presente no servidor, ignore-o.

VMware vCenter SOAP API Settings (Configurações de VMware vCenter SOAP API)

O menu "**VMware vCenter SOAP API Settings**" (Configurações de VMware vCenter SOAP API) fornece as credenciais necessárias ao Nessus para autenticação do VMware vCenter por meio do seu próprio SOAP API, uma vez que o acesso SSH foi descontinuado. O API foi projetado para auditoria de hosts do vCenter, mas **não** das máquinas virtuais em funcionamento nos hosts. Este método de autenticação pode ser usado para realizar varredura com credenciais ou auditorias de conformidade.

Opção	Descrição
VMware vCenter host (Host VMware vCenter)	Nome do host ou IP da instalação do vCenter para auditoria.
VMware vCenter port (Porta VMware vCenter)	Porta que o vCenter responde (padrão: 443).
VMware vCenter user name (Nome de usuário VMware vCenter)	Nome do usuário para autenticação. As credenciais podem ser contas do Active Directory (AD) para hosts integrados ou contas locais e a conta deve estar no grupo `root` local. As credenciais de domínio são user@domain e as contas locais são usuário e senha.
VMware vCenter password (Senha VMware vCenter)	Esta senha é enviada de forma insegura e pode ser interceptada por meio de "sniffing" da rede, a menos que um SSL seja especificado.
SSL	Use o SSL para conectar-se ao host.
Verify SSL Certificate (Verificar certificado SSL)	Se um certificado SSL estiver presente no servidor, verifique sua integridade.

VMware vCenter/vSphere Compliance Checks (Verificações de conformidade VMware vCenter/vSphere)

O menu “**VMware vCenter/vSphere Compliance Checks**” (Verificações de conformidade VMware vCenter/vSphere) permite que clientes comerciais enviem arquivos de auditoria do VMware vCenter ou vSphere que serão usados para determinar se um sistema testado atende aos padrões de conformidade especificados. Até cinco políticas podem ser selecionadas ao mesmo tempo.

Wake-on-LAN (Arranque remoto de LAN)

O menu “**Wake-on-LAN**” (WOL - Arranque remoto de LAN) controla os hosts que receberão pacotes "mágicos" WOL antes de realizar uma varredura, além do tempo de espera (em minutos) para a inicialização dos sistemas. A lista de endereços MAC do WOL é inserida por meio de um arquivo de texto enviado com um endereço MAC de host por linha. Por exemplo:

```
00:11:22:33:44:55
aa:bb:cc:dd:ee:ff
[…]
```

Web Application Tests Settings (Configurações de testes de aplicativos da Web)

O menu “**Web Application Tests Settings**” (Configurações de testes de aplicativos da Web) verifica os argumentos das CGIs (Common Gateway Interfaces) remotas descobertas no processo de espelhamento Web ao tentar enviar erros comuns de programação de CGI, como cross-site scripting, inclusão remota de arquivos, execução de comandos, ataques transversais ou injeção de SQL. Ative esta opção marcando a caixa de seleção “Enable Web applications tests” (Ativar testes de aplicativos da Web). Os testes dependem dos seguintes plugins NASL:

- 11139, 42424, 42479, 42426, 42427, 43160 – SQL Injection (abuso de CGI)
- 39465, 44967 – Execução de comandos (abuso de CGI)
- 39466, 47831, 42425, 46193, 49067 – Cross-Site Scripting (abuso de CGI: XSS)
- 39467, 46195, 46194 – Directory Traversal (abuso de CGI)
- 39468 – HTTP Header Injection (abuso de CGI: XSS)
- 39469, 42056, 42872 – Inclusão de arquivo (abuso de CGI)
- 42055 - Formato de string (abuso de CGI)
- 42423, 42054 - Server Side Includes (abuso de CGI)
- 44136 - Manipulação de cookie (abuso de CGI)
- 46196 - XML Injection (abuso de CGI)
- 40406, 48926, 48927 - Mensagens de erro
- 47830, 47832, 47834, 44134 - Outros ataques (abuso de CGI)

Obs.: esta lista de plugins relacionados a aplicativos da Web é atualizada com frequência e pode não estar completa. Os plugins adicionais podem depender das configurações desta opção de preferência.

Opção	Descrição
Maximum run time (min) (Tempo máx. de execução (min))	Esta opção gerencia o tempo (em minutos) usado na execução de testes de aplicativos da Web. O valor inicial desta opção é 60 minutos e se aplica a todas as portas e CGIs de um determinado website. A varredura de websites da rede local com aplicativos pequenos normalmente é realizada em menos de uma hora. No entanto, websites com aplicativos maiores podem exigir um tempo maior.
Try all HTTP methods (Tentar todos os métodos HTTP)	Normalmente, o Nessus só irá realizar os testes com solicitações GET. Esta opção também instruirá o Nessus a usar “POST requests” (solicitações POST) para testes de formulários da Web aprimorados. Normalmente, os testes de aplicativos da Web usarão apenas solicitações GET, a menos que esta opção esteja ativada. Em geral, aplicativos mais complexos usam o método POST quando um usuário envia dados ao aplicativo. Esta configuração permite um teste mais completo, mas pode aumentar consideravelmente o tempo exigido. Se esta opção for selecionada, o Nessus testará cada script/variável com as solicitações GET e POST.
Combinations of arguments values (Combinações de valores dos argumentos)	Esta opção gerencia a combinação de valores dos argumentos usados nas solicitações de HTTP. Este menu suspenso tem três opções: **one value (um valor)** – Testa um parâmetro por vez com um string de ataque sem

	tentar variações de parâmetros adicionais "sem ataque". Por exemplo: o Nessus tentaria aplicar "`/test.php?arg1=XSS&b=1&c=1`", onde "b" e "c" permitem outros valores, sem testar cada combinação. Este é o método mais rápido de teste com o menor conjunto de resultados gerados. **All pairs (slower but efficient)** (Todos os pares (lento, mas eficiente) – Esta forma de teste é um pouco mais lenta, mas é mais eficaz que o teste "one value" (um valor). Ao verificar diversos parâmetros, verifica também a string de ataque, as variações de uma única variável e usa o primeiro valor com todas as outras variáveis. Por exemplo: o Nessus tenta aplicar "`/test.php?a=XSS&b=1&c=1&d=1`" e percorre as variáveis, de modo que uma receba a string de ataque e a outra redefina todos os valores possíveis (conforme descoberto durante o processo de espelhamento), e qualquer outra variável recebe o primeiro valor. Neste caso, o Nessus nunca testará "`/test.php?a=XSS&b=3&c=3&d=3`" quando o primeiro valor de cada variável for "1". **All combinations (extremely slow)** (Todas as combinações (extremamente lento) – Este método de testes realiza um teste completo de todas as combinações possíveis de sequências de ataque com entrada válida nas variáveis. Enquanto o teste "All-pairs" (Todos os pares) cria um conjunto menor de dados para maior desempenho, esta opção é bastante lenta, pois usa um conjunto completo de dados de testes. Esse método de testes pode levar **muito tempo** para ser concluído.
HTTP Parameter Pollution (Poluição de parâmetro HTTP)	Ao realizar testes de aplicativos da Web, esta opção tenta contornar qualquer mecanismo de filtragem por meio da injeção de conteúdo em uma variável enquanto fornece a mesma variável com conteúdo válido. Por exemplo: um teste de injeção SQL normal pode ter o seguinte aspecto: "`/target.cgi?a='&b=2`". Com a opção HTTP Parameter Pollution (HPP - Poluição de parâmetro HTTP) ativada, a solicitação pode parecer a seguinte: "`/target.cgi?a='&a=1&b=2`".
Stop at first flaw (Parar na primeira falha)	Esta opção determina um ataque em uma nova falha. Isto é feito no nível do script. A detecção de uma falha de XSS não desativará as pesquisas de injeção de SQL ou injeção de cabeçalho, mas haverá, no máximo, um relatório para cada tipo em uma determinada porta, a menos que "thorough tests" (testes completos) esteja definido. Observe que várias falhas do mesmo tipo (por exemplo: XSS, SQLI etc.) podem ser relatadas às vezes, se forem detectadas pelo mesmo ataque. O menu suspenso tem quatro opções: **per CGI** (por CGI) – Assim que uma falha é encontrada em uma CGI por um script, o Nessus passa à CGI conhecida seguinte no mesmo servidor ou, se não houver outras CGIs, à porta/servidor seguinte. Esta é a opção padrão. **per port** (quicker) (por porta (mais rápida) – Assim que uma falha é encontrada em um servidor da Web por um script, o Nessus para e alterna para o outro servidor da Web em uma porta diferente. **per parameter (slow)** (por parâmetro (lenta) – Quando um tipo de falha é encontrado em um parâmetro de uma CGI (por exemplo: XSS), o Nessus alterna para o parâmetro seguinte da mesma CGI ou da CGI conhecida ou para a porta/servidor seguinte. **look for all flaws (slower)** – Executa testes completos, independentemente das falhas encontradas. Esta opção pode gerar um relatório muito detalhado e, na maioria dos casos, não é recomendável.
Test Embedded Web servers (Testar servidores	Os servidores Web incorporados são, muitas vezes, estáticos e não contêm scripts de CGI personalizáveis. Além disso, os servidores Web incorporados podem travar ou

Web incorporados)	deixar de responder quando passam por uma varredura. A Tenable recomenda que os servidores Web incorporados sejam examinados separadamente de outros servidores Web com esta opção.
URL for Remote File Inclusion (URL para inclusão remota de arquivo)	Durante testes de inclusão remota de arquivos (RFI), esta opção especifica um arquivo em um host remoto para ser usado nos testes. Por padrão, o Nessus usará um arquivo seguro hospedado no servidor da Web da Tenable para os testes de RFI. Se o scanner não tiver acesso à Internet, recomenda-se usar um arquivo hospedado internamente para realizar testes mais precisos de RFI.

Web mirroring (Espelhamento Web)

O menu “**Web Mirroring**” (Espelhamento Web) define os parâmetros de configuração para o utilitário original de espelhamento de conteúdo do servidor da Web do Nessus. O Nessus realiza o espelhamento do conteúdo da Web para aprimorar a análise de vulnerabilidades e ajudar a reduzir o impacto sobre o servidor.

Se os parâmetros de espelhamento Web forem definidos de maneira a espelhar um site inteiro, o aumento significativo do tráfego poderá ocorrer durante a varredura. Por exemplo: se houver 1 gigabyte de material em um servidor Web e o Nessus estiver configurado para espelhar todo o conteúdo, a varredura irá gerar pelo menos 1 gigabyte de tráfego do servidor para o scanner Nessus.

Opção	Descrição
Number of pages to mirror (Número de páginas a serem espelhadas)	Número máximo de páginas a espelhar.

Maximum depth (Profundidade máxima)	Limita o número de links que o Nessus seguirá em cada página inicial.
Start page (Página inicial)	O URL da primeira página a ser verificada. Se forem necessárias várias páginas, use dois pontos para separá-las (por exemplo: “/:/php4:/base”).
Excluded items regex (Itens regex excluídos)	Permite que partes do website não estejam sujeitas ao rastreamento. Por exemplo: para excluir o diretório “/manual” e todas as CGIs Perl, defina esse campo como: `(^/manual)|(\.pl(\?.*)?$)`.
Follow dynamic pages (Seguir páginas dinâmicas)	Se esta opção for selecionada, o Nessus seguirá os links dinâmicos e pode exceder os parâmetros definidos acima.

Windows Compliance Checks (Verificações de conformidade Windows)

O menu “**Windows Compliance Checks**” (Verificações de conformidade Windows) permite que clientes comerciais enviem arquivos de auditoria do Microsoft Windows que serão usados para determinar se um sistema testado atende aos padrões de conformidade especificados. Até cinco políticas podem ser selecionadas ao mesmo tempo.

Windows File Contents Compliance Checks (Verificações de conformidade de conteúdos de arquivos do Windows)

O menu “**Windows File Contents Compliance Checks**” (Verificações de conformidade de conteúdos de arquivos do Windows) permite que clientes comerciais enviem arquivos de auditoria do Windows que pesquisam tipos específicos de conteúdos no sistema (por exemplo: cartões de crédito, números de documentos de identidade) para ajudar a determinar o cumprimento de normas internas da empresa ou normas externas.

Quando todas as opções forem configuradas da maneira desejada, clique em “**Submit**” (Enviar) para salvar a política e voltar à guia Policies (Políticas). A qualquer momento, clique em “**Edit**” (Editar) para fazer alterações em uma política criada ou clique em “**Delete**” (Excluir) para excluir completamente uma política.

Para obter mais informações

A Tenable tem vários documentos que descrevem a instalação, implementação, configuração, operação do usuário e testes gerais do Nessus. Os documentos estão listados a seguir:

- **Nessus 5.2 Installation and Configuration Guide (Guia de instalação e configuração do Nessus 5.2)** – instruções passo a passo da instalação e da configuração.
- **Nessus Credential Checks for Unix and Windows (Verificações de Credenciais do Nessus para Unix e Windows)** – informações sobre como realizar varreduras autenticadas de rede com o scanner de vulnerabilidades Nessus.
- **Nessus Compliance Checks (Verificações de Conformidade do Nessus)** – guia geral para compreender e executar verificações de conformidade com o Nessus e o SecurityCenter.
- **Nessus Compliance Checks Reference (Referência de Verificações de Conformidade do Nessus)** – guia completo da sintaxe das verificações de conformidade do Nessus.
- **Nessus v2 File Format (Formato de arquivo Nessus v2)** – descreve a estrutura do formato de arquivo `.nessus`, que foi introduzido com o Nessus 3.2 e NessusClient 3.2.
- **Nessus 5.0 REST Protocol Specification (Especificação do protocolo REST do Nessus 5.0)** – descreve o protocolo e a interface REST do Nessus.
- **Nessus 5 and Antivirus (Nessus 5 e antivírus)** – destaca como vários pacotes de softwares de segurança populares interagem com o Nessus, além de fornecer dicas e soluções para permitir que o software coexista melhor sem comprometer a segurança ou dificultar as ações de varredura de vulnerabilidades
- **Nessus 5 and Mobile Device Scanning (Nessus 5 e varredura de dispositivos móveis)** – descreve como o Nessus integra-se ao Microsoft Active Directory e aos servidores de gerenciamento de dispositivos móveis para identificar dispositivos móveis em uso na rede
- **Nessus 5.0 and Scanning Virtual Machines** (**Nessus 5.0 e a varredura de máquinas virtuais)** – descreve como o scanner Nessus de vulnerabilidades da Tenable Network Security pode ser usado para auditoria da configuração de plataformas virtuais, assim como os softwares em execução nelas
- **Strategic Anti-malware Monitoring with Nessus, PVS, and LCE (Monitoramento estratégico antimalware com Nessus, PVS e LCE)** – descreve como a plataforma USM da Tenable pode detectar uma variedade de softwares maliciosos, além de identificar e determinar a extensão das contaminações por malwares
- **Patch Management Integration (Integração com gerenciamento de patches)** – o documento descreve como o Nessus e o SecurityCenter podem explorar as credenciais nos sistemas de gerenciamento de patches IBM TEM, Microsoft WSUS e SCCM, VMware Go e Red Hat Network Satellite para realizar a auditoria de patches nos sistemas dos quais as credenciais podem não estar disponíveis ao scanner Nessus
- **Real-Time Compliance Monitoring (Monitoramento de Conformidade em Tempo Real)** – descreve como as soluções da Tenable podem ser usadas para ajuda a cumprir muitos tipos diferentes de normas do governo e do setor financeiro.
- **Tenable Products Plugin Families (Famílias de plugins dos produtos Tenable)** – fornece a descrição e o resumo das famílias de plugins para Nessus, Log Correlation Engine e Passive Vulnerability Scanner
- **SecurityCenter Administration Guide (Guia de administração SecurityCenter)**

Outros recursos on-line estão listados a seguir:

- Nessus Discussions Forum (Fórum de Discussão do Nessus): https://discussions.nessus.org/
- Tenable Blog (Blog da Tenable): http://www.tenable.com/blog
- Tenable Podcast (Podcast da Tenable): http://www.tenable.com/podcast
- Example Use Videos (Vídeo de exemplos de uso): http://www.youtube.com/user/tenablesecurity
- Tenable Twitter Feed (Feed do twitter da Tenable): http://twitter.com/tenablesecurity

Entre em contato conosco pelo e-mail support@tenable.com, sales@tenable.com ou visite nosso site no endereço http://www.tenable.com/.

Sobre a Tenable Network Security

A Tenable Network Security conta com a confiança de mais de 20 mil empresas, incluindo todo o Departamento de Defesa dos EUA, além de diversas das maiores empresas do mundo e governos, para manter-se à frente das vulnerabilidades, ameaças e riscos de conformidade emergentes. Suas soluções, Nessus e SecurityCenter, continuam a definir o padrão para identificar vulnerabilidades, evitar ataques e estar em conformidade com uma ampla variedade de requisitos normativos. Para mais informações, visite www.tenable.com.

SEDE GLOBAL

Tenable Network Security
7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046
410.872.0555
www.tenable.com